
FONDO PROVINCIA



ESPOSIZIONE

DELLA

TEORICA DELLE SOSTITUZIONI

PER

GIUSEPPE JANNI

PROFESSORE DI GEOMETRIA ANALITICA NELLA REGIA SCUOLA DI MARINA

Estratto dal Giornale di Matematiche ad uso degli Studenti delle Università italiane.



NAPOLI
STABILIMENTO TIPOGRAFICO DI A. TRANI
Vico Conte di Mola, 13

1871



PREFAZIONE

Lo scopo principale dell' Algebra è la risoluzione dell'equazioni. Questo problema fu risoluto da Lagrange con un metodo applicabile solo all'equazioni dei quattro primi gradi, non per difetto di generalità, ma sibbene per l'impossibilità di risolvere l'equazioni di un grado maggiore del quarto.

Abel prendendo le mosse da questa impossibilità, da lui la prima volta dimostrata, cercò le condizioni a cui deve soddisfare un equazione per essere risolubile mediante radicali, e pervenne al teorema: che un equazione è risolubile per radicali quando una delle sue radici è funzione di un altra.

Era naturale che il genio di Galois che seguì immediatamente Abel avesse generalizzate le sue ricerche; ed infatti, poggiandosi sul principio che ogni equazione ammette un gruppo di sostituzioni fatte sulle radici nel quale si riflettono tutte le sue proprietà, stabilì una teoria completa diretta a fissare i caratteri dell'equazioni risolubili per mezzo di altre di gradi inferiori.

Volendomi mettere in possesso di questa teoria la quale forma la parte più interessante dell'Algebra moderna ho preso a studiare il pregevolissimo trattato delle sostituzioni di Jordan il quale coordina sapientemente al commento dei risultati di Galois le sue particolari ricerche e tutti i lavori fatti sulle sostituzioni dagl' insigni geometri Lagrange—Canchy—Betti—Brioschi—Mathieu—Hermite—Serret—Kronecher.

Questo lavoro consistente in una redazione dei due primi libri dell'opera di Jordan è lo scarso frutto dei miei primi studî su questo soggetto. Esso è diviso in tre parti: nella prima si tratta delle sostituzioni e dei gruppi in generale: nella seconda si espongono le nozioni sulle congruenze che hanno più attinenza colle sostituzioni lineari: nella terza si parla delle sostituzioni esprimibili analiticamente, ed in particolar modo delle lineari.

Il lettore sia cortese di usarmi il suo compatimento, trattandosi di teoriche che presentano un immensa difficoltà.

PARTE PRIMA

DELLE SOSTITUZIONI IN GENERALE.

CAPO 1.°

Nozioni preliminari.

1. Dicesi *sostituzione* l'operazione con cui da una permutazione di più lettere si passa ad un'altra permutazione delle medesime lettere. Così, per passare dalla permutazione *abcd* delle quattro lettere *a*, *b*, *c*, *d* all'altra *acdb*, bisogna scambiare *b* con *c*, *c* con *d*, e *d* con *b*; quindi questi scambii costituiscono una sostituzione che si rappresenta col simbolo

$$\binom{acdb}{abcd}.$$

2. Se sulla permutazione *abcd* si opera la sostituzione

$$A = \binom{acdb}{abcd},$$

si avrà l'altra *acdb*, su cui operando la sostituzione

$$B = \binom{bdca}{abcd},$$

si avrà la permutazione *bcad* la quale si ottiene altresì dalla proposta, operandovi la sostituzione

$$C = \binom{bcad}{abcd}.$$

Quest'ultima sostituzione, che produce lo stesso effetto che si ottiene operando prima la sostituzione A e poi la B, si chiama *prodotto* dell'altre due, e si scrive

$$AB = C.$$

In generale s'intende per *prodotto* di più sostituzioni A, B, C etc. la sostituzione che, operata sopra una data permutazione, dà lo stesso risultato che si ottiene, se sulla medesima permutazione prima si opera la sostituzione A, poi la B, indi la C e così di seguito. Di qui risulta il significato che debba annettersi ad una potenza di una data sostituzione. Infine indicheremo con A^{-1} la sostituzione inversa di A; per modo che operando su di una data permutazione prima A e poi A^{-1}, o viceversa, la permutazione non si altera; ossia che il prodotto di A per A^{-1} è la sostituzione identica che ad una lettera sostituisce la medesima lettera; quindi, indicando con 1 questa sostituzione, si ha $AA^{-1}=1$.

3. Due sostituzioni si dicono tra loro *mutabili*, se operando sopra una permutazione una qualunque di esse e poi l'altra, si ha sempre lo stesso risultato; per modo che indicando con A e B queste sostituzioni, sarà

$$AB = BA.$$

È evidente che due sostituzioni che spostano lettere diverse siano tra loro mutabili Così saranno mutabili le sostituzioni

$$\binom{abdc}{abcd}, \quad \binom{bacd}{abcd}.$$

4. Una sostituzione che in una data permutazione sostituisce a ciascuna lettera la seguente, ed all'ultima la prima chiamasi *circolare:* così sarebbe circolare la sostituzione

$$A_1 = \binom{bcdea}{abcde}.$$

Si è dato questo nome ad una tale sostituzione, perchè dividendo una circonferenza, nel caso particolare di A_1 in cinque parti uguali, indi scrivendo in un punto di divisione la lettera a e negli altri successivi ordinatamente b, c, d, e, se si fa girare la circonferenza di un angolo uguale a $\frac{2\pi}{5}$, i posti occupati primitivamente da a, b, c, d, e saranno occupati rispettivamente da b, c, d, e, a.

La suddetta sostituzione A_1 si rappresenta anche con uno qualunque dei simboli

$$(abcde), \ (bcdea), \ (cdeab), \ (deabc), \ (eabcd),$$

che si ottengono ponendo in 1° luogo una per volta le cinque lettere, in 2° luogo quella che deve rimpiazzare la 1ª, in 3° luogo quella che deve rimpiazzare la 2ª; e così di seguito.

5. *Una sostituzione che non è circolare equivale al prodotto di più sostituzioni circolari.*

Infatti questa sostituzione scambierà una lettera a con un altra b, poi la b con un altra c. e così seguitando s'incontrerà necessariamente una lettera l, che sarà scambiata con a; quindi la sostituzione proposta opererà sulle lettere a, b, c, ... l la sostituzione circolare $(a, b, c ... l)$. Similmente un altra lettera h, non contenuta nelle precedenti, darà luogo ad un altra sostituzione circolare, e così di seguito. Per esempio la sostituzione

$$\binom{bcdfac}{abcdef}$$

equivale al prodotto delle due sostituzioni circolari

$$(abc), \quad (cdf);$$

per modo che sarà

$$\binom{bcdfac}{abcdef} = (abc)\,(cdf).$$

Le sostituzioni circolari che costituiscono una sostituzione qualunque si chiamano *cicli* di questa sostituzione.

È d'avvertirsi che una sostituzione può non spostare una o più lettere; allora ciascuna di queste lettere costituisce un ciclo: così sarà

$$\binom{bcadef}{abcdef} = (abc)\,(d)\,(e)\,(f) = (abc).$$

6. Poichè una sostituzione circolare di n lettere equivale a far girare di un angolo uguale a $\frac{2\pi}{n}$ la circonferenza che, divisa in n parti uguali, porta scritte le n lettere nei punti di divisione; ripetendo m volte di seguito questa sostituzione, ciascuna lettera sarà rimpiazzata da quella che ne dista per un arco uguale ad $m\frac{2\pi}{n}$; quindi bisogna ripeterla almeno n volte perchè ogni lettera riprendesse il suo posto: perciò la potenza n^a di una sostituzione circolare di n lettere è la minima potenza di questa sostituzione che sia uguale ad 1. Ora la potenza n^a di una sostituzione qualunque è uguale al prodotto delle potenze n^e dei suoi cicli. Infatti consideriamo la sostituzione $A=(abc)(def)$: sarà

$$A^2=(abc)(def)(abc)(def);$$

ma poichè le sostituzioni (abc), (def) sono tra loro mutabili, sarà ancora

$$A^2=(abc)(abc)(def)(def)=(abc)^2(def)^2.$$

Ma il grado della minima potenza di una sostituzione circolare che sia uguale ad 1 è dinotato dal numero delle sue lettere, dunque, se indichiamo con ω, ω' etc. i numeri delle lettere che compongono i cicli di una sostituzione non circolare, il minimo multiplo di ω, ω' etc. indicherà il grado della minima potenza di questa sostituzione che sia uguale ad 1.

Laonde, se chiamiamo *ordine* di una sostituzione il grado della minima potenza di questa sostituzione che sia uguale ad 1, possiamo dire che l'ordine di una sostituzione circolare è uguale al numero delle sue lettere; e l'ordine di una sostituzione non circolare è il minimo multiplo degli ordini dei suoi cicli.

7. Una sostituzione si dice *primitiva* quando il suo ordine è un numero primo o la potenza di un numero primo.

Teorema 1.° — *Ogni sostituzione non primitiva è uguale al prodotto di più sostituzioni primitive.*

Sia A una sostituzione di ordine $D=p^\alpha q^\beta r^\gamma$, essendo p, q, r numeri primi. Poichè A^D è la minima potenza di A che sia uguale ad 1, gli ordini delle sostituzioni

$$A_1=A^{\frac{D}{p^\alpha}},\quad A_2=A^{\frac{D}{q^\beta}},\quad A_3=A^{\frac{D}{r^\gamma}}$$

saranno rispettivamente p^α, q^β, r^γ, perciò saranno primitive. Ora, essendo p^α e $q^\beta r^\gamma$ primi tra loro, possiamo trovare due numeri interi l ed m' positivi o negativi che soddisfano alla condizione

$$lq^\beta r^\gamma+m'p^\alpha=1.$$

Similmente, essendo q^β ed r^γ primi tra loro, si possono trovare due numeri interi m ed n che soddisfano alla condizione

$$m'=mr^\gamma+nq^\beta.$$

Sostituendo questo valore di m' nell'altra uguaglianza, si ha

$$lq^\beta r^\gamma+mp^\alpha r^\gamma+np^\alpha q^\beta=1,$$

ovvero
$$l\frac{D}{p^\alpha}+m\frac{D}{q^\beta}+n\frac{D}{r^\gamma}=1;$$

laonde sarà
$$A_1{}^l A_2{}^m A_3{}^n = A^{l\frac{D}{p^\alpha}+m\frac{D}{q^\beta}+n\frac{D}{r^\gamma}} = A.$$

8. Se A e B sono due sostituzioni, l'altra $B^{-1}AB$ si chiama la *trasformata* di A per mezzo di B o con B.

Teorema 2.° — *Si ottiene la trasformata di* A *con* B, *sostituendo a ciascuna lettera di ciascun ciclo di* A *quella che ad essa fa succedere* B.

Sia $A=(abcd)\,(efg)$, e supponiamo che B scambii a, b, c, d, e, f, g rispettivamente con $a', b', c', d', e', f', g'$. La sostituzione $B^{-1}AB$ equivale ad operare prima B^{-1}, poi A ed infine B: ma B^{-1}, essendo inversa di B, scambia $a', b', c', d', e', f', g'$ rispettivamente con a, b, c, d, e, f, g; indi la sostituzione A rimpiazza quest'ultime lettere rispettivamente coll'altre b, c, d, a, f, g, e; infine la B cambia quest'ultime rispettivamente nell'altre $b', c', d', a', f', g', e'$: dunque $B^{-1}AB$ produce nelle lettere a', b', c', d', e', f' le due sostituzioni circolari (a', b', c', d'), (e', f', g'). Ma l'altre lettere che entrano in B, ricevendo per B^{-1} e per B due spostamenti contrarii, restano ferme per la sostituzione $B^{-1}AB$; dunque sarà
$$B^{-1}AB=(a'b'c'd')\,(e'f'g').$$

9. Si chiamano *simili* due sostituzioni quando hanno il medesimo numero di cicli, ed i cicli corrispondenti sono del medesimo ordine. Da questa definizione e dal teorema precedente si deduce che una sostituzione è simile alla sua trasformata con una sostituzione qualunque.

Teorema 3.° — *Se* A e B *sono due sostituzioni simili contenenti* μ *cicli di ordine* m, μ' *di ordine* m' *e così di seguito, vi sono*
$$1\cdot 2\ldots\mu m^{\mu}\cdot 1\cdot 2\ldots\mu' m'^{\mu'}\ldots$$
sostituzioni colle quali trasformando A, *si ottiene* B.

Infatti i cicli di una sostituzione possono cambiare di posto, senza che si alteri la sostituzione; perchè i cicli sono sostituzioni relative a lettere diverse, quindi sono mutabili tra loro. Laondo permutando in tutt'i modi possibili i cicli dello stesso ordine di B, si avranno $1\cdot 2\ldots\mu\times 1\cdot 2\ldots\mu'\ldots$ forme diverse di B, nelle quali i cicli corrisponderanno a quelli di A. Inoltre ad ogni lettera di un ciclo possiamo fare occupare il 1° posto, variando convenevolmente i posti dell'altre lettere dello stesso ciclo; quindi se si fa quest'operazione in ciascun ciclo delle diverse forme di B, si otterranno
$$1\cdot 2\ldots\mu\cdot m^{\mu}\times 1\cdot 2\ldots\mu'\cdot m^{\mu'}\times\ldots$$
sfrme diverse di B, nelle quali i cicli si corrisponderanno con quelli di A. Ora la sostituzione, che scambia le lettero di ciascun ciclo di A colle lettere corrispondenti del ciclo corrispondente di una qualunque delle forme di B, trasforma A in B: dnnque vi sono
$$1\cdot 2\ldots\mu\cdot m^{\mu}\times 1\cdot 2\ldots\mu'\cdot m'^{\mu'}\times\ldots$$
oostituzioni diverse che trasformano A in B.

CAPO 2.°

Dei gruppi in generale.

10. Un sistema di sostituzioni forma un *gruppo* quando contiene il prodotto di due qualunque di esse.

Si dice *ordine* di un gruppo il numero delle sostituzioni che lo compongono, e *grado* il numero delle lettere spostate dalle sue sostituzioni.

11. *Se* A *è una sostituzione ed* m *è il suo ordine, le sostituzioni* $1, A, A^2 \ldots A^m$ *formano un gruppo.*

Infatti il prodotto di due qualunque di esse A^p, A^q è A^{p+q}; ovvero, indicando con r il resto della divisione di $p+q$ per m, sarà $A^{m+r} = A^m \cdot A^r$: ma $A^m = 1$; dunque $A^p \cdot A^q = A^r$; ma, essendo r minore di m, A^r appartiene alla suindicata serie; dunque anche il prodotto $A^p \cdot A^q$ appartiene alla stessa.

12. *Le sostituzioni che trasformano una data sostituzione* A *in se stessa formano un gruppo.*

Infatti siano A_1 ed A_2 due di queste sostituzioni: la trasformata di A con $A_1 A_2$ sarà

$$(A_1 A_2)^{-1} A A_1 A_2 :$$

ma, dovendo essere $(A_1 A_2)^{-1} A_1 A_2 = 1$; sarà $(A_1 A_2)^{-1} = A_2^{-1} A_1^{-1}$: quindi sarà

$$(A_1 A_2)^{-1} A A_1 A_2 = A_2^{-1} A_1^{-1} A A_1 A_2 :$$

ma $A_1^{-1} A A_1 = A$ per ipotesi; dunque sarà

$$(A_1 A_2)^{-1} A A_1 A_2 = A_2^{-1} A A_2 ;$$

ma $A_2^{-1} A A_2 = A$ per ipotesi; dunque il prodotto $A_1 A_2$ trasforma A in se stessa. Quindi il sistema delle sostituzioni che trasformano A in se stessa contiene il prodotto di due qualunque di esse.

13. *Le trasformate delle sostituzioni* A,B etc. *di un gruppo con una sostituzione qualunque* M *formano un gruppo che dicesi il gruppo trasformato del dato con* M.

Infatti il gruppo dato, contenendo le sostituzioni A e B, conterrà il loro prodotto AB; quindi il sistema delle trasformate conterrà le tre sostituzioni

$$M^{-1} AM , \quad M^{-1} BM , \quad M^{-1} ABM ;$$

ma

$$M^{-1} ABM = M^{-1} AM \; M^{-1} BM ;$$

perchè $MM^{-1} = 1$; dunque il sistema delle trasformate conterrà il prodotto di due di esse.

Se il gruppo formato dalle trasformate si confonde col dato, si dice che M sia *permutabile* al gruppo dato.

14. *Le sostituzioni permutabili ad un gruppo* H *formano un gruppo.*

Siano M ed N due sostituzioni permutabili al gruppo H ed A una sostituzione di questo: inoltre si abbia

$$M^{-1} AM = A_1 \quad , \quad N^{-1} AN = A_2 :$$

saranno A_1 ed A_2 sostituzioni di H. Ora si ha

$$(MN)^{-1}AMN = N^{-1}M^{-1}AMN = N^{-1}A_1N = A_2;$$

dunque il sistema delle sostituzioni permutabili ad H contiene il prodotto di due di esse.

15. *Se si combinano per moltiplicazione in tutt' i modi possibili più sostituzioni* A, B, C etc. *e le loro potenze, le sostituzioni che risultano formano un gruppo che dicesi derivato dalle sostituzioni* A, B, C etc. *e s' indica col simbolo* (A, B, C...).

È evidente che questo sistema contenga il prodotto di due sostituzioni che ad esso appartengono.

16. *Se* M *è una sostituzione permutabile ad un gruppo* G, *le derivate da* M *e dalle sostituzioni di* G *possono mettersi sotto una delle forme* $M^{\alpha}g_{\alpha}$, $g_{\beta}M^{\beta}$: *essendo* g_{α} *e* g_{β} *due sostituzioni di* G.

Sia $M^pg_1M^q$ una sostituzione derivata da M e dalla sostituzione g_1 di G. Possiamo metterla sotto la forma $M^{p-1}\cdot Mg_1M^{-1}MM^q$: ma Mg_1M^{-1} è una sostituzione di G; quindi indicandola con g_2, la proposta si può mettere sotto la forma $M^{p-1}g_2M^{q+1}$. Seguitando ad operare allo stesso modo si possono riunire con M^q tutt' i fattori di M^p, e così la proposta sostituzione prenderà la forma g_2M^{p+q}. Si potrebbero ugualmente riunire i fattori di M^q a quelli di M^p, ed allora la sostituzione prenderebbe la forma $M^{p+q}g_{\beta}$.

17. Teorema 1.° — *Se un gruppo* H *è contenuto in un altro* G, *l' ordine* n *di* H *è un divisore dell' ordine di* G, **N**.

Questo teorema è dovuto a Lagrange.

Siano

$$1, S_1, S_2, S_3 \ldots\ldots S_{n-1}$$

le sostituzioni di H e Σ una sostituzione di G non contenuta in H. Le sostituzioni

$$\Sigma, S_1\Sigma, S_2\Sigma \ldots\ldots S_{n-1}\Sigma$$

saranno contenute in G, differiranno tra loro, e saranno distinte da quelle di H; poichè se fosse $S_p\Sigma = S_q$, sarebbe $\Sigma = S_p^{-1}S_q$, e quindi Σ apparterrebbe ad H, il che è contro l'ipotesi. Laonde se G non contiene altre sostituzioni sarà $N = 2n$. Ma se G contiene un'altra sostituzione Σ_1 diversa da quelle contenute nelle due serie precedenti, avrà anche l' altre

$$\Sigma_1, S_1\Sigma_1, S_2\Sigma_1 \ldots\ldots S_{n-1}\Sigma_1$$

le quali sono diverse tra loro e da quelle di H: inoltre differiscono da quelle della 2.ª serie; perchè se fosse $S_p\Sigma_1 = S_q\Sigma$, sarebbe $\Sigma_1 = S_p^{-1}S_q\Sigma$; ma $S_p^{-1}S_q$ è una sostituzione di H, quindi Σ_1 sarebbe uguale ad una sostituzione di H moltiplicata per Σ, perciò apparterrebbe alla 2.ª serie, il che è contrario all' ipotesi. Dunque N sarà almeno uguale a $3n$. Se N è maggiore di $3n$ si dimostrerebbe similmente che almeno sarebbe uguale a $4n$, e così di seguito.

Da questa dimostrazione risulta che le sostituzioni di G possono essere disposte in un quadro come il seguente

$$\begin{array}{llll} 1 & S_1 & S_2 & \ldots\ldots\ldots\ S_{n-1} \\ \Sigma & S_1\Sigma & S_2\Sigma & \ldots\ldots\ldots\ S_{n-1}\Sigma \\ \Sigma_1 & S_1\Sigma & S_2\Sigma_1 & \ldots\ldots\ldots\ S_{n-1}\Sigma_1 \\ \vdots & \vdots & & \qquad\qquad\ \vdots \end{array}$$

o come nell'altro

$$\begin{array}{llll} 1 & S_1 & S_2 & \ldots\ldots\ldots\ S_{n-1} \\ \Sigma & \Sigma S_1 & \Sigma S_2 & \ldots\ldots\ldots\ \Sigma S_{n-1} \\ \Sigma_1 & \Sigma_1 S_1 & \Sigma_1 S_2 & \ldots\ldots\ldots\ \Sigma_1 S_{n-1} \\ \vdots & \vdots & & \qquad\qquad\ \vdots \end{array}$$

Corollario 1.° — L'ordine di un gruppo di k lettere divide il prodotto $1 \cdot 2 \cdot 3 \ldots k$.

Poichè questo gruppo è contenuto nell'altro formato da tutte le sostituzioni di k lettere che sono $1 \cdot 2 \cdot 3 \ldots k$.

Corollario 2.° — L'ordine di un gruppo che contiene una sostituzione di ordine p è divisibile per p.

Poichè questo gruppo contiene l'altro formato dalle potenze delle sostituzioni di ordine p.

18. Teorema 2.° — *Se l'ordine di un gruppo non è divisibile per un numero primo* p, *esso non può contenere alcuna sostituzione di ordine* p.

Questo teorema è dovuto a Cauchy, e si poggia sopra i due seguenti lemmi.

Lemma 1.° — Siano $G = (g_1\, g_2 \ldots)$, $H = (h_1\, h_2 \ldots)$, $U = (u_1\, u_2 \ldots)$ tre gruppi rispettivamente di ordine M, N, P; e siano i due primi contenuti nel 3°: il numero delle sostituzioni di U che non soddisfano alla condizione $g_\alpha u_a = u_a h_\beta$ è un multiplo di MN.

Sia u_a una sostituzione che non soddisfa la detta condizione; dico che non vi soddisferanno le MN sostituzioni contenute nella formola $g_\alpha u_a h_\beta$. Infatti se si avesse

$$g_\gamma g_\alpha u_a h_\beta = g_\alpha u_a h_\beta h_\lambda\,,$$

si avrebbe

$$g_\alpha^{-1} g_\gamma g_\alpha u_a = u_a h_\beta h_\lambda h_\beta^{-1};$$

ma $g_\alpha^{-1} g_\gamma g_\alpha$, $h_\beta h_\lambda h_\beta^{-1}$ appartengono rispettivamente ai gruppi G ed H; quindi u_a soddisferebbe alla condizione in parola: il che è contro l'ipotesi. Inoltre le sostituzioni della forma $g_\alpha u_a h_\beta$ sono tutte distinte, poichè se si avesse

$$g_\alpha u_a h_\beta = g_{\alpha'} u_a h_{\beta'}\,,$$

sarebbe

$$g_{\alpha'}^{-1} g_\alpha u_a = u_a h_{\beta'} h_\beta^{-1},$$

il che non è. Adunque il numero delle sostituzioni di U che non soddisfano alla condizione $g_\alpha u_a = u_a h_\beta$ è almeno MN.

Se questo numero è maggiore di MN, sia $u_{a'}$ un'altra sostituzione di U che non soddisfa la detta condizione: allora non vi soddisferanno le MN sostituzioni comprese nella formola $g_\alpha u_{a'} h_\beta$. Queste ultime sostituzioni sono tra loro distinte,

e lo sono anche dalle altre $g_\alpha u_a h_\beta$; poichè se fosse

$$g_\alpha u_a h_\beta = g_{\alpha'} u_{a'} h_{\beta'},$$

sarebbe $$g_{\alpha'}^{-1} g_\alpha u_a h_\beta h_{\beta'}^{-1} = u_{a'};$$

ma $g_{\alpha'}^{-1} g_\alpha$ ed $h_\beta h_{\beta'}^{-1}$ appartengono rispettivamente ai gruppi G ed H, quindi $u_{a'}$ sarebbe una delle sostituzioni contenute nella espressione $g_\alpha u_a h_\beta$, il che non è. Adunque il numero delle sostituzioni di U che non soddisfano alla condizione $g_\alpha u_a = u_a h_\beta$ è almeno 2MN. Se questo numero superasse 2MN si dimostrerebbe similmente che dovrebbe essere uguale almeno a 3MN, e così di seguito.

Corollario — Se G non contiene alcuna sostituzione simile a qualcuna delle sostituzioni di H, tutte le sostituzioni di U non soddisfano alla condizione $g_\alpha u_a = u_a h_\beta$, poichè se questa uguaglianza avesse luogo, si avrebbe anche l'altra $u_\alpha^{-1} g_a u_a = h_\beta$, quindi H conterrebbe la sostituzione h_β simile a g_α, il che è contrario all'ipotesi: quindi l'ordine P di U è divisibile per MN.

19. Lemma 2.° — Se p è un numero primo e p^f è la massima potenza di p contenuta nel prodotto $1 \cdot 2 \ldots k$, si può sempre formare con k lettere un gruppo di ordine p^f.

Se $k < p$, sarà $f = 0$ e $p^f = 1$; allora il gruppo formato dalla sola sostituzione 1 soddisferà alla condizione enunciata.

Quindi basterà dimostrare che se la proposizione enunciata nel lemma è vera per tutt'i valori di k minori di p^v, lo sia anche per tutt'i valori di k maggiori di p^v e minori di p^{v+1}.

Indicando con q un numero minore di p^v e con r un altro minore di p, ogni numero k maggiore di p^v e minore di p^{v+1} sarà espresso dalla formola $k = pq + r$.

Consideriamo pq delle k lettere e dividiamole nei q sistemi

$$a_1, a_2, a_3, \ldots a_p; \quad b_1, b_2, b_3, \ldots b_p, \ldots;$$

ciascuno composto di p lettere. Indichiamo con $S_1, S_2 \ldots S_p$ le sostituzioni circolari di ordine p, formate rispettivamente dalle lettere del primo sistema, da quelle del secondo, e così di seguito. Inoltre siano t_1, t_2, t_3 etc. delle sostituzioni che scambiano le lettere di un sistema colle corrispondenti di un altro sistema; e $T = (t_1, t_2, t_3 \text{ etc.})$ un gruppo di ordine p^γ, essendo p^γ la massima potenza di p contenuta in $1 \cdot 2 \cdot 3 \ldots q$.

Le derivate da S_1, S_2 etc. e dalle sostituzioni di T possono mettersi sotto la forma $t_m S^\alpha S_1^\beta \ldots$: infatti sia $S^\alpha t_m S^\beta$ una di queste derivate; essa può scriversi sotto la forma $t_m t_m^{-1} S^\alpha t_m S^\beta$; ma se t_m scambia le lettere del 1° sistema con quelle del 2°, $t_m^{-1} S^\alpha t_m$ è uguale ad S_1^α; quindi la derivata in parola si può mettere sotto la forma $t_m S_1^\alpha S^\beta$, ovvero sotto l'altra $t_m S^\beta S_1^\alpha$, perchè S ed S_1, permutando lettere diverse, sono tra loro mutabili.

Ma se nell'espressione $t_m S^\alpha S_1^\beta \ldots$ si danno ad m tutt'i valori da 1 sino a p^γ e ad α, β etc. tutt'i valori da 1 a p, si otterranno sostituzioni diverse. Infatti se si avesse

$$t_m S^\alpha S_1^\beta \ldots = t_{m'} S^{\alpha'} S_1^{\beta'} \ldots;$$

si avrebbe anche $$t_{m'}^{-1} t_m = S^{\alpha'} S_1^{\beta'} \ldots S^{-\alpha} S_1^{-\beta} \ldots$$

ma il 1° membro dinota una sostituzione che scambia le lettere di alcuni sistemi colle corrispondenti di altri sistemi, mentre il 2° membro dinota una sostituzione che permuta tra loro le lettere appartenenti ad un medesimo sistema; dunque quest'uguaglianza non può aver luogo se non nel caso che ambedue i membri siano uguali ad 1; perciò sarà $m = m'$ ed

$$S^{\alpha}S_1^{\beta}\ldots = S^{\alpha'}S_1^{\beta'}\ldots$$

donde

$$S^{\alpha-\alpha'} = S_1^{\beta'-\beta}\ldots :$$

ma il 1° membro dinota una sostituzione che sposta le lettere del 1° sistema, mentre il 2° membro dinota una sostituzione che permuta le lettere degli altri sistemi; dunque dovrà essere $\alpha = \alpha'$; similmente si dimostrerebbe $\beta = \beta'$ etc.

Adunque il gruppo L, formato dalle sostituzioni derivate $t_m S^{\alpha} S_1^{\beta}\ldots$ è dell'ordine $p^{\gamma}\cdot p^q = p^{\gamma+q}$. Ma questa potenza di p è appunto la massima potenza di p contenuta nel prodotto $1\cdot2\cdot3\ldots k$. Infatti, essendo $k = pq + r$, ed essendo r minore di p, il massimo intero contenuto in k è q; quindi i fattori del precedente prodotto, divisibili per p, sono i seguenti

$$p,\ 2p,\ 3p\ldots qp;$$

perciò la massima potenza di p contenuta in detto prodotto sarà la massima potenza di p contenuta nell'altro

$$1\cdot2\cdot3\ldots q\cdot p^q;$$

ma la massima potenza di p contenuta in $1\cdot2\ldots q$ è per ipotesi p^{γ}; dunque la massima potenza di p contenuta nel prodotto $1\cdot2\ldots k$ è $p^{\gamma+q}$. Quindi l'esistenza del gruppo L dimostra l'enunciata proposizione.

20. Premessi questi due lemmi veniamo alla dimostrazione del teorema.

Sia H un gruppo che non contenga alcuna sostituzione di ordine p: esso non conterrà alcuna sostituzione il cui ordine sia divisibile per p; poichè se contenesse la sostituzione A di ordine pk, essendo $A^{pk} = 1$, sarebbe $(A^k)^p = 1$, e quindi H conterrebbe la sostituzione A^k di ordine p, il che è contrario all'ipotesi. Il gruppo L avendo per ordine $p^{\gamma+q} = p^f$, ogni sua sostituzione avrà per ordine un numero che divide p^f e quindi divisibile per p; per conseguenza ciascuna delle sue sostituzioni deve avere almeno un ciclo il cui ordine sia un multiplo di p; ma nessuna sostituzione di H può avere un ciclo il cui ordine sia divisibile per p, dunque nessuna delle sostituzioni di H può essere simile a qualcuna di quelle di L. Ma L ed H sono contenuti nel gruppo I formato da tutte le sostituzioni possibili di k lettere. Dunque, in forza del corollario del 1° lemma, l'ordine $1\cdot2\cdot3\ldots k$ di I deve essere divisibile pel prodotto dell'ordine M di H per l'ordine p^f di L; quindi M deve dividere $\frac{1\cdot2\ldots k}{p^f}$; ma questo numero non contiene più fattori uguali a p, dunque neppure M dovrà contenere tali fattori, per conseguenza se l'ordine di un gruppo non è divisibile per p esso non potrà contenere una sostituzione di ordine p.

CAPO 3.°

Gruppo alternato.

21. Una sostituzione che scambia tra loro due lettere dicesi *trasposizione*.

Una sostituzione circolare di p lettere $a, b, c...$ è il prodotto di $p-1$ trasposizioni (ab), (ac)...; quindi una sostituzione di k lettere contenente n cicli sarà il prodotto di $k-n$ trasposizioni.

22. Teorema 1.° — *Il numero delle trasposizioni che contiene il prodotto di due sostituzioni* S e T *è pari o impari, secondochè è pari o impari la somma* $\alpha+\beta$ *dei numeri* α e β *di trasposizioni di cui esse si compongono.*

Supponiamo che sia $S=(abcde)(fg)$. Moltiplichiamo S per la trasposizione (ac) formata da due lettere esistenti nel medesimo ciclo. Se si opera la sostituzione $(abcde)(fg)(ac)$ sulla permutazione $abcdefg$ si ottiene il risultato $badecgf$, che si otterrebbe ancora se sopra $abcdefg$ si operasse la sostituzione $(ab)(cde)(fg)$; quindi sarà

$$S(ac)=(ab)(cde)(fg).$$

E poichè $S(ac)$ contiene un ciclo di più di S, il numero delle trasposizioni di $S(ac)$ sarà $\alpha-1$.

Or supponiamo che si moltiplichi S per la trasposizione (af) formata da due lettere esistenti in cicli diversi. Operando la sostituzione $S(af)$ sulla permutazione $abcdefg$, si ha l'altra $bcdefga$, la quale si otterrebbe anche se si operasse sulla permutazione $abcdefg$ la sostituzione $(abcdefg)$; quindi sarà

$$S(af)=(abcdefg).$$

E poichè $(abcdefg)$ contiene un ciclo di meno di S, equivale ad $\alpha+1$ trasposizioni. Ma la differenza tra $\alpha+1$ ed $\alpha+1$ è zero, e quella tra $\alpha+1$ ed $\alpha-1$ è 2, dunque il numero delle trasposizioni che contiene il prodotto di S per una trasposizione è $\equiv\alpha+1 \pmod 2$. Di qui risulta, che indicando con $\alpha_1, \alpha_2 ... \alpha_\beta$ i numeri di trasposizioni che presentano i prodotti di S per la 1ª trasposizione di T, per le due prime, e così di seguito, sarà

$$\alpha_1\equiv\alpha+1 \pmod 2,\quad \alpha_2\equiv\alpha_1+1 \pmod 2 \ldots \alpha_\beta\equiv\alpha_{\beta-1}+1 \pmod 2;$$

quindi, addizionando e sopprimendo i termini comuni ai due membri, si avrà

$$\alpha_\beta\equiv\alpha+\beta \pmod 2.$$

Corollario. — Le sostituzioni di un gruppo G, costituite da un numero pari di trasposizioni, formano un gruppo H. Poichè il prodotto di due di esse, constando di un numero pari di trasposizioni e dovendo appartenere a G, fanno parte di H.

Teorema 2.° — *Se in un gruppo* G *vi sono delle sostituzioni equivalenti ad un numero impari di trasposizioni, e delle altre ad un numero pari, l'ordine del gruppo* H *formato da queste ultime è la metà dell'ordine di* G. *Ed* H *è permutabile alle sostituzioni di* G.

Se indichiamo con $S_1, S_2, \ldots$ le sostituzioni di H e con T una sostituzione di G, formata da un numero impari di trasposizioni, le sostituzioni

$$S_1, S_2 \ldots; \quad TS_1, TS_2, \ldots \qquad (1)$$

saranno distinte. Infatti, essendo tra loro distinte $S_1, S_2 \ldots$, lo saranno anche l'altre $TS_1, TS_2 \ldots$ Inoltre una delle $S_1, S_2 \ldots$ non può essere eguale ad una delle $TS_1, TS_2 \ldots$; poichè se fosse $S_3 = TS_4$, sarebbe $S_3 S_4^{-1} = T$, e quindi T apparterrebbe ad H, il che non è. Ma le (1) rappresentano tutte le sostituzioni di G. Poichè se una sostituzione U di G è formata da un numero pari di trasposizioni, essa è contenuta nella serie $S_1, S_2 \ldots$, e se è formata da un numero impari di trasposizioni, l'altra $T^{-1}U$, equivalendo ad un numero pari di trasposizioni, appartiene alla serie $S_1, S_2 \ldots$; perciò $TT^{-1}U = U$ fa parte della serie $TS_1, TS_2 \ldots$ Adunque l'ordine di G è doppio di quello di H.

Or se indichiamo con S_n una sostituzione qualunque di H, e con α, β, γ i numeri delle trasposizioni che compongono U, S_n, $U^{-1}S_nU$, poichè il numero delle trasposizioni di U^{-1} è $\equiv -\alpha \pmod 2$, sarà

$$V \equiv -\alpha + \beta + \alpha \pmod 2:$$

ma β è pari, dunque lo sarà anche V, perciò $U^{-1}S_nU$ appartiene ad H: laonde, contenendo H la trasformata di una qualunque delle sue sostituzioni per mezzo di una sostituzione di G, sarà ogni sostituzione di G permutabile ad H.

Corollario 1.° — *Tutte le sostituzioni di* k *lettere, equivalenti ad un numero pari di trasposizioni, formano un gruppo* H' *al quale sono permutabili tutte le sostituzioni delle* k *lettere.* H' *si chiama gruppo alternato.*

Corollario 2.° — *Se un gruppo* G *di* k *lettere contiene il gruppo alternato, o si confonde con esso, o contiene tutte le sostituzioni che si possono formare colle* k *lettere.*

Poichè se G contiene altre sostituzioni oltre quelle del gruppo alternato, indicando con N l'ordine di questo gruppo, quello di G sarà 2N; ed il numero delle sostituzioni possibili con k lettere è appunto 2N.

23. Teorema 3.° — *Ogni sostituzione del gruppo alternato è il prodotto di sostituzioni circolari di 3.° ordine.*

Sia $S = (abcd)(ef)$ una sostituzione del gruppo alternato. Poichè $(abcd) = (abc)(ad)$, sarà

$$S = (abc)(ad)(ef):$$

ma $\quad (ad)(ef) = (ad)(ae)(ea)(ef), \quad (ad)(ae) = (ade), \quad (ea)(ef) = (eaf),$

quindi sarà $\quad S = (abc)(ade)(eaf).$

24. Teorema 4.° — *Un gruppo* G, *al quale ogni sostituzione è permutabile, contiene il gruppo alternato, se il numero* k *delle sue lettere è superiore a* 4.

Poichè ogni sostituzione formata colle k lettere di G è permutabile a G; questo gruppo conterrà tutte le sostituzioni simili ad una delle sue sostituzioni, S.

$S_1, S_2, S_3 \ldots S_n$ le sostituzioni di G. Allora le sostituzioni

$$\left.\begin{array}{llll} S_1, & S_2, & S_3, \ldots\ldots & S_n \\ TS_1, & TS_2, & TS_3, \ldots\ldots & TS_n \\ T^{-1}S_1, & T^{-1}S_2, & T^{-1}S_3, \ldots\ldots & T^{-1}S_n \end{array}\right\} \qquad (1)$$

sono distinte. Infatti, essendo distinte quelle della 1ª linea, lo saranno quelle della 2ª, come anche quelle della 3ª. Inoltre una della 2ª linea non può essere eguale ad un altra della 1ª; poichè se fosse $TS_m = S_{m'}$, sarebbe $T = S_{m'} S_m^{-1}$, e quindi T farebbe parte di G, il che non è. Similmente una della 3ª linea non può confondersi con un altra della 1ª; poichè se fosse $T^{-1}S_m = S_{m'}$, sarebbe $T^{-1} = S_{m'}S_m^{-1}$, e quindi $(T^{-1})^2 = (S_{m'} S_m^{-1})^2$; ma

$$(T^{-1})^2 = T^{-3} \cdot T = T,$$

quindi sarebbe $T = (S_{m'} S_m^{-1})^2$, e T apparterrebbe a G, il che non è. Infine una della 2ª linea non può eguagliare un'altra della terza; poichè se fosse $T^{-1}S_m = TS_{m'}$, sarebbe $T^2 T^{-1} S_m = T^3 S_{m'}$, ossia $TS_m = S_{m'}$, il che si è dimostrato impossibile. Ma le (1) al più costituiscono tutte le sostituzioni possibili, dunque G contiene al più il terzo di queste sostituzioni.

CAPO 4.°

Gruppi transitivi.

26. Un gruppo dicesi *transitivo* quando per le sue sostituzioni una lettera qualunque può esser posta nel sito occupato da una lettera determinata. Nel caso contrario un gruppo dicesi *intransitivo*.

In generale un gruppo dicesi m volte *transitivo*, quando per le sue sostituzioni m lettere qualunque possono simultaneamente esser poste nei siti primieramente occupati da m lettere determinate.

Da questa definizione si deduce, che colle sostituzioni di un gruppo G, m volte transitivo, si possono scambiare m lettere qualunque con altre m lettere qualunque. Infatti sia S una sostituzione di G che scambii m lettere qualunque $a', b', c' \ldots$ colle m lettere determinate $a, b, c, \ldots$, ed S_1 un'altra sostituzione di G che scambii altre m lettere qualunque $a'', b'', c'', \ldots$ con $a, b, c, \ldots$. G contiene la sostituzione SS_1^{-1} la quale prima scambia $a', b', c' \ldots$ con $a, b, c \ldots$, ed indi $a, b, c, \ldots$ con $a'', b'', c'', \ldots$; quindi scambia $a', b', c', \ldots$ con $a'', b'', c'' \ldots$.

27. *Un gruppo di* m *lettere è transitivo*, *se contiene una sostituzione circolare formata da queste* m *lettere*. Poichè con questa sostituzione e colle sue diverse potenze si può scambiare una lettera qualunque con un'altra determinata.

Come pure un gruppo di m *lettere è* n *volte transitivo, se contiene una sostituzione circolare di ordine* m, *un'altra di ordine* $m-1$, *un'altra di ordine* $m-2$, *e così di seguito sino ad una sostituzione di ordine* $m-n+1$. Poichè colla 1ª sostituzione o con una delle sue potenze si può scambiare una lettera qua-

lunque con quella che non entra nella 2ª sostituzione; indi con questa o con una delle sue potenze si può scambiare una 2ª lettera qualunque con quella che entra nella 2ª e non nella 3ª; e così seguitando si possono scambiare m lettere qualunque con m lettere determinate.

28. Teorema 1.° — *Le lettere di un gruppo intransitivo* G *si possono dividere in sistemi tali che le sue sostituzioni permutano tra loro le lettere di ciascun sistema.*

Poichè G è intransitivo, le sue sostituzioni non possono scambiare con una lettera determinata ciascuna delle rimanenti; perciò supponiamo che le sole lettere $a_1, a_2, a_3 \ldots$ si scambiino con a; allora ciascuna lettera del sistema $a, a_1, a_2 \ldots$ si scambierà con un'altra del medesimo sistema; poichè, se supponiamo che la sostituzione S di G scambii a_1 con l, ed indichiamo con S_1 la sostituzione che scambia a_1 con a, l'altra $S^{-1}S_1$, scambiando prima l con a_1 ed indi a_1 con a, scambierà l con a, e quindi l dovrà far parte del sistema $a, a_1, a_2 \ldots$ Similmente se le sole lettere $b_1, b_2, b_3 \ldots$ si scambiano con b, le sostituzioni di G permuteranno tra loro le lettere $b, b_1, b_2, \ldots$, e così di seguito.

Corollario 1.° — Quindi le sostituzioni di G saranno della forma ABC...; A'B'C'...;... essendo A, A'... delle sostituzioni sopra le lettere $a, a_1, a_2 \ldots$; B, B'... delle sostituzioni sopra le lettere $b, b_1, b_2, \ldots$; e così di seguito. E poichè la permutazione delle lettere $a, a_1, a_2 \ldots$ fatta dal prodotto delle sostituzioni ABC..., A'B'C'... è indicata da AA', così le sostituzioni A, A'... formano un gruppo, il quale è transitivo; perchè per le sue sostituzioni a può rimpiazzare una qualunque delle altre lettere del sistema $a, a_1, a_2 \ldots$ Lo stesso è delle sostituzioni B, B'..., delle altre C, C'..., e così di seguito.

Corollario 2.° — *Se i sistemi* $a, a_1, a_2 \ldots, b, b_1, b_2, \ldots, \ldots$ *sono formati rispettivamente di* $\alpha, \alpha', \alpha''$ *etc. lettere, l'ordine di* G *dividerà il prodotto* $1 \cdot 2 \ldots \alpha \times 1 \cdot 2 \ldots \alpha' \times 1 \cdot 2 \ldots \alpha'' \ldots$ Infatti si moltiplichi ciascuna delle sostituzioni che si possono formare colle lettere del 1° sistema per ciascuna di quelle che si possono formare colle lettere del 2° sistema; indi ciascuno di questi prodotti si moltiplichi per ciascuna delle sostituzioni che si possono formare colle lettere del 3° sistema, e così di seguito sino alle sostituzioni formate colle lettere dell'ultimo sistema; si avrà così un gruppo G' il cui ordine è $1 \cdot 2 \ldots \alpha \times 1 \cdot 2 \ldots \alpha' \times 1 \cdot 2 \ldots \alpha'' \times \ldots$; ma G' contiene G, dunque l'ordine di G divide il suddetto prodotto (17).

29. Teorema 2.° — *Se* m *indica il numero di sistemi di posizioni diverse che le sostituzioni di un gruppo* G *possono dare a determinate lettere* a, b, c, etc., *ed* n *dinota l'ordine del gruppo formato dalle sostituzioni di* G *che non spostano* a, b, c etc., *sarà* mn *l'ordine di* G.

Siano $1, p_1, p_2 \ldots p_{n-1}$ le sostituzioni di G che non spostano le lettere a, b, c, etc., e sia S una sostituzione di G che pone queste lettere in uno degli m sistemi di posizioni possibili; allora anche l'altre $Sp_1, Sp_2 \ldots Sp_{n-1}$ le collocheranno secondo lo stesso sistema di posizioni in cui le pone S. Or dico che

$$S,\ Sp_1,\ Sp_2 \ldots Sp_{n-1} \qquad (1)$$

siano le sole che soddisfano a questa condizione. Infatti, indichiamo con R una so-

stituzione di G, diversa da S, e che colloca a, b, c, etc. negli stessi posti in cui le mette S: la sostituzione $S^{-1}R$ lascia immobili queste lettere; perchè dinotando con a', b', c' etc. le lettere che occupano i posti nei quali R ed S costituiscono $a, b, c...$, S^{-1} scambia $a, b, c...$ con $a', b', c'...$, ed indi R scambia a', b', c' etc. con $a, b, c...$; quindi $S^{-1}R$ è uguale ad una delle sostituzioni $1, p_1, p_2...$: supponiamo che sia $S^{-1}R = p_m$; allora sarà $R = Sp_m$, e quindi R sarà contenuta nella serie (1). Or corrispondendo a ciascuno degli m sistemi di posizioni delle lettere a, b, c, etc. n sostituzioni di G, saranno mn le sostituzioni di G.

Corollario. — Se un gruppo G di m lettere è n volte transitivo, le sue sostituzioni possono far prendere ad n lettere determinate tanto posizioni diverse quante sono le disposizioni ad n ad n di m lettere, ossia $m(m-1)...(m-n+1)$; quindi l'ordine di G sarà divisibile per $m(m-1)...(m-n+1)$.

30. Teorema 3.° — *Se un gruppo G non contiene il gruppo alternato ed è n volte transitivo, ciascuna delle sue sostituzioni deve spostare più di n lettere.*

Supponiamo che G contenga la sostituzione S che sposta le n lettere $a, b, c...$ Essendo G n volte transitivo, conterrà una sostituzione T che scambia queste lettere con altre n lettere qualunque $\alpha, \beta, \gamma...$; perciò conterrà anche la sostituzione TST^{-1} che rappresenta una qualunque delle sostituzioni simili ad S, e quindi conterrà il gruppo H, formato da tutte le sostituzioni simili ad S. Ma questo gruppo è permutabile a tutte le sostituzioni possibili; dunque H e G conterranno il gruppo alternato; ma questo è contrario all'ipotesi, dunque è impossibile che G contenga una sostituzione che sposta n lettere. Questo teorema è dovuto a Matthieu e conduce all'altro

31. Teorema 4.° — *Se un gruppo G non contiene il gruppo alternato, ed è n volte transitivo, ciascuna delle sue sostituzioni deve spostare più di* 2n − 4 *lettere.*

Supponiamo che G contenga la sostituzione $S = (abc...)(def...)(g...)$ la quale sposti q lettere, essendo $q < m-3$; e siano $a, b ... d, e, f$ le prime n lettere di questa sostituzione. Poichè G è n volte transitivo, conterrà una sostituzione che lascia immobili le lettere $a, b, c ... d, e$, e scambia f con φ: supponiamo che la medesima sostituzione scambi g con γ. Allora G conterrà

$$T^{-1}ST = (abc...)(de\varphi...)(\gamma...),$$

come anche

$$T^{-1}STS^{-1} = (abc...)(de\varphi...)(\gamma...)(abc...)^{-1}(def...)^{-1}(g...)^{-1}.$$

Ora in quest'ultima sostituzione lo spostamento indicato dal ciclo $(abc...)$ è distrutto da quello indicato dal ciclo $(ab...)^{-1}$; inoltre se è

$$abc...def...g...\varphi...\gamma...$$

una permutazione delle lettere di G, essa pel ciclo $(de\varphi...)$ diverrà

$$abc...e\varphi f...dg...\lambda...\gamma...;$$

indi pel ciclo $(def...)^{-1}$ diverrà

$$abc...d\varphi e...g...\lambda...\gamma...;$$

quindi la lettera d ritiene il suo posto in seguito alle operazioni indicate dai due

cicli in cui entra d; laonde per la sostituzione $T^{-1}STS^{-1}$ non mutano posto le $n-2$ lettere $a, b \dots d$; ma ciascuna delle due sostituzioni S^{-1} e $T^{-1}ST$ sposta q lettere ed e è comune ad entrambe; quindi $T^{-1}STS^{-1}$ sposterà un numero di lettere indicato da $q' = 2q - 2(n-2) + 1 = 2q - (2n-3)$; ma q è minore di $2n-3$, dunque sarà $q' < q$.

Similmente da quest'ultima sostituzione che sposta q' lettere si può passare ad un'altra che sposta un numero q'' di lettere, minore di q'; e così seguitando si giungerà ad una sostituzione che sposta n lettere; ma questo pel teorema precedente è impossibile, quindi G non può contenere alcuna sostituzione che sposti meno di $2n-3$ lettere.

Corollario 1.° — *Se s'indica con* k *il numero delle lettere di* G *e con* m *il più grande dei due numeri* n *e* 2n − 4, *l'ordine di* G *deve dividere* $\frac{1 \cdot 2 \cdot 3 \dots k}{1 \cdot 2 \cdot 3 \dots m}$.

Poichè ogni sostituzione di G sposta un numero di lettere maggiore del più grande dei due numeri n e $2n-3$, G non conterrà alcuna sostituzione simile a quella del gruppo H, formato da tutte le sostituzioni di m lettere. Ma H e G sono contenuti nel gruppo G′, formato da tutte le sostituzioni di k lettere, dunque l'ordine di G′ deve esser divisibile (18, Co.) pel prodotto degli ordini di G e di H, ma l'ordine di G′ è $1 \cdot 2 \cdot 3 \dots k$, e quello di H è $1 \cdot 2 \cdot 3 \dots m$, dunque $\frac{1 \cdot 2 \cdot 3 \dots k}{1 \cdot 2 \cdot 3 \dots m}$ deve esser divisibile per l'ordine di G.

Corollario 2.° — *Se un gruppo* G *di* k *lettere è* n *volte transitivo*, n *non può superare il più piccolo dei due numeri* $\frac{k+4}{3}$ e $\frac{k}{2}$.

Essendo G n volte transitivo, il suo ordine deve essere divisibile pel prodotto $k(k-1) \dots (k-n+1)$, ma esso deve dividere $\frac{1 \cdot 2 \cdot 3 \dots k}{1 \cdot 2 \cdot 3 \dots m}$, quindi $1 \cdot 2 \cdot 3 \dots k$ deve essere divisibile pel prodotto $1 \cdot 2 \dots m(k-n+1) \dots (k-1)k$; perciò m non deve superare $k-n$; ma m è il più grande dei numeri $2n-4$ ed n; quindi se questo è n, dovrà essere $n < k-n$, donde $n < \frac{k}{2}$; e se $m = 2n-4$, sarà $2n-4 < k-n$, donde $n < \frac{k+4}{3}$.

32. Teorema 5.° — *Un gruppo* G *permutabile alle sostituzioni di un gruppo* H, n *volte transitivo, è almeno* n − 1 *volte transitivo.*

Sia $S = (abc\dots)(def\dots)$ una sostituzione di G, e siano $a, b, c \dots d, e, f$ le prime n lettere in essa contenute. H, essendo n volte transitivo, conterrà una sostituzione T che lascia immobili $a, b, c \dots e$, e scambia f con p. Inoltre G, per essere permutabile a tutte le sostituzioni di H, dovrà contenere la trasformata di S per mezzo di T, ossia $T^{-1}ST = (abc\dots)(dep\dots)$; e quindi conterrà anche

$$S^{-1}T^{-1}ST = (abc\dots)^{-1}(def\dots)^{-1}(abc\dots)(dep\dots).$$

In questa sostituzione le operazioni indicate dai due cicli $(abc\dots)^{-1}$, $(abc\dots)$, come contrarie, si distruggono, quindi per operare la sostituzione $S^{-1}T^{-1}ST$ sopra la permutazione

$$abc\dots def\dots lp\dots$$

delle lettere di G basta operarvi l'altra $(def...)^{-1}$ $(dep...)$; ma eseguendo la sostituzione $(def...)^{-1}$; si ha

$$abc \ldots lde \ldots gp \ldots ,$$

e facendo in seguito l'operazione $(dep \ldots)$, si ha

$$abc \ldots lep \ldots kq \ldots ;$$

dunque $S^{-1}T^{-1}ST$ non sposta le $n-2$ lettere $a, b \ldots e$, e scambia f con p; per modo che dovrà contenere un ciclo in cui le lettere f e p sono contigue; quindi potrà essere rappresentata da

$$U = (fp \ldots) \ldots$$

Ora H, essendo n volte transitivo, conterrà una sostituzione V che scambia le n lettere $a, b, c \ldots e, f, p$ con n lettere qualunque $\alpha, \beta, \gamma \ldots \varepsilon, \varphi, \pi$; quindi G conterrà la sostituzione $V^{-1}UV$ che lascia immobili le $n-2$ lettere $\alpha, \beta, \gamma \ldots \varepsilon$ e scambia φ con una lettera qualunque π; quindi G deve essere almeno una volta transitivo. Ora G, essendo transitivo, conterrà una sostituzione R_1 che scambia una lettera qualunque con α; ma il gruppo formato dalle sostituzioni di G che non spostano α, essendo transitivo, contiene una sostituzione R_2 che scambia una lettera qualunque, diversa da α, con β; quindi G conterrà la sostituzione R_1R_2 che scambia due lettere qualunque coll'altre α e β. Similmente il gruppo formato dalle sostituzioni di G che non spostano α e β è transitivo; quindi contiene una sostituzione R_3 che scambia una lettera qualunque diversa da α e da β coll'altra γ; perciò G conterrà la sostituzione $R_1R_2R_3$ che scambia tre lettere qualunque con α, β, γ; e così seguitando a ragionare si perviene al risultato: che G debba contenere una sostituzione $R_1R_2 \ldots R_{n-2}$ che scambia $n-2$ lettere qualunque coll'altre $\alpha, \beta, \gamma \ldots \delta$, ma il gruppo formato dalle sostituzioni di G che non spostano quest'ultima lettera è anche transitivo, quindi deve contenere una sostituzione R_{n-1} che scambia una lettera qualunque, diversa dalle suindicate, con ε; perciò G conterrà la sostituzione $R_1R_2 \ldots R_{n-2}R_{n-1}$ che scambia simultaneamente $n-1$ lettere qualunque con $n-1$ lettere determinate; dunque G è almeno $n-1$ volte transitivo.

Corollario. — *Il gruppo alternato di* k *lettere non può contenere un altro gruppo al quale le sue sostituzioni sono permutabili, se* $k > 4$.

Il gruppo alternato è $k-1$ volte transitivo; quindi se contenesse un gruppo H al quale le sue sostituzioni fossero permutabili, H sarebbe almeno $k-2$ volte transitivo; ma esse, al più, è tante volte transitivo quante sono l'unità contenute nel minore dei due numeri $\frac{n+4}{3}$ e $\frac{k}{2}$, il quale è minore di $k-2$, quando $k > 4$; dunque è impossibile che il gruppo alternato contenga un altro gruppo al quale le sue sostituzioni sono permutabili.

Se $k = 4$, il gruppo formato dalle sostituzioni che si deducono da (ab) (cd) sono permutabili a tutte le sostituzioni possibili; quindi con più ragione lo sono a quelle del gruppo alternato.

CAPO 5.°

Gruppi transitivi in cui l'ordine uguaglia il grado.

33. Teorema 1.° — *In un gruppo transitivo* G, *nel quale l'ordine uguaglia il grado, ad ogni ciclo di una sua sostituzione corrisponde una divisione delle lettere in sistemi tali, che per ogni sostituzione di* G *le lettere di un sistema si scambiano con quelle di un altro sistema.*

Poichè il gruppo G è transitivo, il suo ordine deve essere uguale al grado moltiplicato pel numero delle sostituzioni che non spostano una data lettera (29), ma l'ordine ed il grado di G sono uguali, dunque G contiene una sola sostituzione la quale non sposta una data lettera, la quale è 1; perciò ogni sostituzione di G sposta tutte le lettere. Di qui risulta che in G non vi possono essere due sostituzioni che scambiano una data lettera con un'altra data; poichè, moltiplicando l'una per l'inversa dell'altra, si avrobbe una sostituzione, diversa dall'unità, la quale non sposterebbe una lettera, il che è impossibile.

Or sia $(a, a_1, a_2, \dots a_{m-1})$ un ciclo di una sostituzione A di G. Poichè questo gruppo è transitivo, conterrà una sostitusione B cho ad a farà succedere un'altra lettera b, non contenuta nol suddetto ciclo. Siano $b_1, b_2 \dots b_{m-1}$ le lettere che la medesima sostituzione farà succedere rispettivamente ad $a_1, a_2 \dots a_{m-1}$. Quest'ultime sono differenti dalle precedenti. Infatti supponiamo che sia $a_\nu = b_\mu \cdot A^{\nu-\mu}$ contiene il ciclo.

$$(a, a_1, a_2 \dots a_{m-1})^{\nu-\mu} = (a \dots a_\mu, a_\nu \dots);$$

quindi fa succedere a_ν ed a_μ, ossia b_μ ed a_μ, ma anche B fa succedere b_μ ad a_μ, dunque G conterrebbe due sostituzioni che scambierebbero a_μ con b_μ, il che è impossibile. Sia c un'altra lettera di G, diversa da quelle contenute nei sistemi

$$a, a_1, a_2 \dots a_{m-1}; \quad b, b_1, b_2 \dots b_{m-1}.$$

G conterrà una sostituzione C che ad a farà succedero c. Supponiamo che C scambi $a_1, a_2 \dots a_{m-1}$ rispettivamente con $c_1, c_2 \dots c_{m-1}$. Quest'ultime lettere saranno diverse da quelle contenute nel duo sistemi precedenti; poichè, se fosse $b_\nu = c_\mu$, vi sarebbero le due sostituzioni B ed $A^{\mu-\nu}C$ che farebbero succedere c_μ ad a_ν, il che è impossibile. Seguitando a ragionare nello stesso modo si divideranno tutte le lettere di G in sistemi, ciascuno di m lettere. Or se S è una sostituzione di G che fa succedere c_μ a b_ν, essa scambierà $b_\nu, b_{\nu+1} \dots b_{\nu-1}$ rispettivamente con $c_\mu, c_{\mu+1} \dots c_{\mu-1}$. Invero B^{-1} fa succedere a $b, b_1, b_2 \dots b_{m-1}$ rispettivamente $a, a_1, a_2 \dots a_{m-1}$, ed a queste ultime lettere $A^{\mu-\nu}$ fa succedere rispettivamente l'altre $a_{\mu-\nu}, a_{\mu-\nu+1} \dots a_{\mu-\nu+m-1}$, le quali per C si scambiano rispettivamente con $c_{\mu-\nu}, c_{\mu-\nu+1} \dots c_{\mu-\nu+m-1}$; quindi $B^{-1}A^{\mu-\nu}C$ scambia $b_\nu, b_{\nu+1} \dots b_{\nu-1}$ rispettivamente con $c_\mu, c_{\mu+1} \dots c_{\mu-1}$. Ma G non può contenere due sostituzioni diverse che fanno succedere l'una all'altra due lettore date, dunque S e $B^{-1}A^{\mu-\nu}C$, cho scambiano b_ν con c_μ, debbono essere identiche, e quindi S scambierà $b_\nu, b_{\nu+1} \dots b_{\nu-1}$ rispettivamente con $c_\mu, c_{\mu+1} \dots c_{\mu-1}$.

Corollario — *Se si forma una sostituzione, prendendo per suoi cicli i diversi sistemi di lettere della divisione originata da un ciclo di una sostituzione qualunque di G, per esempio*

$$\sigma = (aa_1 \ldots a_{m-1})(bb_1 \ldots b_{m-1})(cc_1 \ldots c_{m-1}) \ldots ,$$

sarà σ mutabile con tutte le sostituzioni di G.

Infatti se S sostituisce c_μ a b_ν, sostituirà $c_{\mu+1}$ a $b_{\nu+1}$, ma σ scambia b_ν con $b_{\nu+1}$, quindi σS scambierà b_ν con $c_{\mu+1}$. Similmente σ sostituendo $c_{\mu+1}$ a c_μ, Sσ prima scambierà b_ν con c_μ ed indi c_μ con $c_{\mu+1}$, per modo che scambierà b_ν con $c_{\mu+1}$, ma b_ν è una lettera qualunque, dunque sarà σS = Sσ.

34. Teorema 2.° — *Il gruppo G' derivato da tutte le sostituzioni analoghe a σ; 1° è transitivo; 2° ciascuna delle sue sostituzioni sposta tutte le lettere; 3° contiene tutte le sostituzioni mutabili con quelle di G.*

1.° G' è *transitivo*. Poichè, se k è una lettera qualunque, G conterrà una sostituzione che a k farà succedere una data lettera a; perciò questa sostituzione conterrà un ciclo in cui queste lettere si succedono, ma questo ciclo fa parte di una sostituzione di G', dunque G' conterrà una sostituzione che ad una lettera qualunque fa succedere una data lettera; quindi G' è transitivo.

2. *Ogni sostituzione di G' sposta tutte le lettere.* Sia σ' una sostituzione di G' che lascia immobile a, e fa succedere k a b, e sia S' una sostituzione di G che scambia a con b. Operando sulla permutazione

$$abc \ldots k \ldots$$

la sostituzione σ'S', si avrà $bk\delta \ldots \varepsilon \ldots$;

ed operando sulla medesima permutazione la sostituzione S'σ', si avrà

$$k\gamma\delta_1 \ldots \varepsilon_1 \ldots ,$$

ma questi due risultati sono diversi, quindi σ'S' sarebbe diversa da S'σ'; perciò σ'' non sarebbe mutabile con S', il che non è.

3.° *Il gruppo G' contiene tutte le sostituzioni mutabili con quelle di G.* Sia P una sostituzione mutabile con quelle di G, e supponiamo che faccia succedere a_1 ad a; essa sarà identica all'altra

$$\sigma = (aa_1 \ldots a_{m-1})(bb_1 \ldots b_{m-1}) \ldots$$

Infatti se Q è la sostituzione di G che contiene il ciclo $(aa_1 \ldots)$, ed indichiamo con k la lettera che P fa succedere ad a_1, PQ farà succedere a_2 ed a, e QP farà succedere k ad a; quindi sarà $k = a_2$. Similmente si dimostrerebbe che P fa succedere a_3 ad a_2, e così di seguito; per modo che P contiene il ciclo $(a, a_1, a_2 \ldots)$. Supponiamo che P faccia succedere x a b, e sia R la sostituzione di G che scambi le lettere $a, a_1, a_2 \ldots$ con $b, b_1, b_2 \ldots$; allora RP farà succedere x ad a, e PR farà succedere b_1 ad a; quindi sarà $x = b_1$. Similmente si dimostrerebbe che P farà succedere b_2 a b_1, e così di seguito; per modo che P contiene il ciclo $(bb_1 \ldots)$. Nello stesso modo si proverebbe che P contiene gli altri cicli $(c, c_1, c_2 \ldots) \ldots$; quindi P è identica a σ.

CAPO 6.°

Gruppi non primitivi.

35. Allorchè le lettere di un gruppo transitivo si possono dividere in sistemi, formati dallo stesso numero di lettere, e tali che per ciascuna sostituzione del gruppo le lettere di ciascun sistema o si permutano tra loro, o si scambiano con quelle di un altro sistema, il gruppo si dice *non primitivo*.

Quando le lettere di un gruppo non comportano la suddetta divisione, esso si dice *primitivo*.

Teorema 1.° — *Sia G un gruppo non primitivo le di cui lettere comportino due divisioni in sistemi tali, che per ciascuna sostituzione di G le lettere di ciascun sistema siano rimpiazzate da quelle di un altro sistema. Indichiamo con S, S′, S″ etc. i sistemi dati dalla 1ª divisione, e con T, T′, T″ etc. quelli dati dalla 2ª. Si formino dei nuovi sistemi* S_1, S'_1, S''_1 etc., *riunendo i sistemi T che hanno delle lettere comuni con uno stesso sistema S. Parimenti si formino degli altri sistemi* T_1, T'_1, T''_1 etc., *frazionando i sistemi S in parti tali, che ciascuna contenga le lettere comuni ad S ed ad un sistema T. I sistemi* T_1 *e gli altri* S_1 *formeranno altre due divisioni in sistemi tali, che per ogni sostituzione di G le lettere di un sistema si scambiano con quelle di un altro sistema.*

Sia a una lettera comune ad S ed T, e b una lettera comune ad S′ ed a T′. Il gruppo G, essendo transitivo, conterrà una sostituzione che scambierà a con b, quindi alle lettere di S sostituirà quella di S′, ed alle lettere di T quelle di T′; laonde scambierà le lettere comuni ad S ed a T con quelle comuni ad S′ ed a T′.

Siano a, a', a''... delle lettere comuni ad S ed a T, T′, T″ etc. e b, b', b''... delle lettere comuni ad S′ ed a T‴, T^{iv}, T^{v} etc. La sostituzione che pone b in luogo di a, porrà b, b', b'' etc. in luogo di a, a', a'' etc.; e quindi ai sistemi T, T′, T″ etc. farà succedere gli altri T‴, T^{iv}, T^{v} etc.

Osservazione. — Se il sistema S contiene tutte le lettere di un sistema T, sarà S formato da due o più sistemi T, poichè, se a è una lettera comune ad S ed a T, e b una lettera comune ad S ed a T′, la sostituzione, che scambia a con b, deve scambiare T con T′, ma colla detta sostituzione si scambiano tra loro le lettere di S; dunque T′ dovrà esser contenuto in S.

Di qui risulta che quando un sistema T è contenuto in un sistema S, le due nuove divisioni coincidono colle proposte.

Se T ha una sola lettera di comune con S, i sistemi T_1 saranno formati da una sola lettera.

Infine se tutt' i sistemi T hanno delle lettere comuni collo stesso sistema S, i sistemi T_1 si ridurranno ad un solo che conterrà tutte le lettere.

36. Teorema 2.° — *Sia G un gruppo non primitivo ed E l'insieme delle sue lettere. Tra le divisioni di queste lettere in sistemi tali che per ciascuna sostitu-*

zione di G le lettere di un sistema si scambiano con quelle di un altro sistema, scegliamo quelle che formano la serie

[E], [S, S'...], [T, T'...], [U, U'...]......[X, X'...] (1).

così condizionata.

1.° *Che non vi sia una divisione in sistemi tali che uno di essi contenga tutte le lettere di* S.

2.° *Che* S *contenga* T, *ma che non vi sia un'altra divisione in sistemi tali, che uno di essi sia contenuto in* S *e contenga* T.

3.° *Che* T *contenga* U, *ma che non vi sia un'altra divisione in sistemi tali, che uno di essi contenga* U *e sia contenuto in* T.

Così di seguito sino all'ultima divisione [X, X'...] *nella quale ciascun sistema è formato da una sola lettera.*

Se vi è una divisione [s, s'...] *non compresa in* (1), *essa apparterrà ad una serie analoga alla* (1).

Poichè ciascun sistema X dell'ultima divisione della (1) è formato da una sola lettera, e questi sistemi X riproducono E e tutti gli altri sistemi della (1), così *s* che si compone di una parte di E dovrà contenere un sistema della (1) ed essere contenuto in un altro della stessa serie. Supponiamo che contenga U e sia contenuto in S. Indichiamo con *t* l'assieme dei sistemi U comuni ad S ed ad *s*. Dico che la serie di divisioni

[E], [s, s'...], [t, t'...], [U, U'...]......[X, X']

sia analoga alla (1).

Invero *t* non può contenere due sistemi U appartenenti allo stesso sistema T, altrimenti con questi sistemi U si potrebbe formare un'altra divisione in sistemi tali, che ciascuno conterrebbe un sistema U e sarebbe contenuto in un sistema T, il che è impossibile. Inoltre *t* non può contenere tutt'i sistemi U che compongono T, altrimenti *s* conterrebbe T, il che è contrario all'ipotesi. Quindi *t* dovrà contenere dei sistemi U che appartengono ai diversi sistemi T che compongono S.

Ora dico che *t* debba contenere un sistema U di ciascuno dei sistemi T che compongono S. Poichè se non li contenesse, si avrebbe un'altra divisione in sistemi tali, che ciascuno sarebbe formato dalle T che hanno un sistema U comune con *t*, e questo sistema conterrebbe T e sarebbe contenuto in S, il che è impossibile.

Infine tra le divisioni [*t*, *t'*...] ed [U, U'...] non vi può essere una divisione intermedia; poichè se vi fosse, un sistema di questa divisione dovrebbe contenere un numero di sistemi U minore di quello che contiene *t*, il che si è dimostrato impossibile.

Il sistema *s* è formato da più sistemi *t*. Due di questi non possono contenere le U delle T dello stesso sistema S, altrimenti vi sarebbe una divisione in sistemi tali, che conterrebbero i sistemi U e sarebbero contenuti nei sistemi T, il che è impossibile. Quindi i sistemi *t* che compongono *s* contengono le U di diversi sistemi S.

Ora dico che *s* debba contenere tanti sistemi *t* quanti sistemi S sono in E, poichè, se fosse altrimenti, riunendo i sistemi S che hanno dei sistemi U comuni

con s, si avrebbero dei sistemi che conterrebbero S e sarebbero contenuti in E, il che è impossibile. Per questa ragione tra s e t non vi può essere un sistema intermedio.

Parimenti tra E ed s non vi è sistema intermedio, poichè se vi fosse, questo dovrebbe contenere più sistemi U appartenenti allo stesso sistema T, e quindi essi formerebbero un sistema che conterrebbe U e sarebbe contenuto in T, il che è impossibile.

Osservazione. — Supponiamo che E contenga k lettere, che E contenga m sistemi S, S n sistemi T, T p sistemi U etc. Allora i numeri delle lettere di S, T, U etc. saranno rispettivamente $\frac{k}{m}$, $\frac{k}{mn}$, $\frac{k}{mnp}$ etc. Ma t contiene n sistemi U, s m sistemi t, quindi i numeri delle lettere di s, t, U etc. saranno $\frac{k}{p}$, $\frac{k}{mp}$, $\frac{k}{mnp}$ etc.

37. Teorema 2.° — *Siano*

$$[E],\ [S,S'...],\ [T,T'...]...[U,U'...]...[X,X'...]$$
$$[E],\ [s,s'...],\ [t,t'...]...[u,u'...]...[x,x'...]$$

due serie di partizioni in sistemi che soddisfano alle condizioni indicate nell' enunciato del teorema precedente.

Siano $k, \frac{k}{\lambda}, \frac{k}{\lambda\mu}, \frac{k}{\lambda\mu\nu}$ etc. *i numeri delle lettere di* E,S,T,U...X; $\frac{k}{l}, \frac{k}{lm}, \frac{k}{lmn}$ etc. *quelli delle lettere di* s, t, u...x; *i fattori* λ, μ, ν etc. *saranno, eccetto nell'ordine, identici agli altri* l, m, n, etc.

Infatti pel teorema precedente possiamo formare una serie di partizioni in sistemi, di cui facesse parte la divisione [s, s'...], ed i fattori fossero λ, μ, ν, etc. Da questa serie si potrebbe passare ad un'altra che contenesse [s, s'...] e [t, t'...] e che avesse anche i fattori λ, μ, ν, etc. e così di seguito.

Corollario. — Da questo teorema risulta che i gruppi non primitivi si possano classificare secondo il numero e la grandezza dei fattori λ, μ, ν, etc., i quali perciò possono chiamarsi fattori di non primitività. Il numero di questi fattori, che è costante, si chiama *grado di non primitività.*

38. Teorema 3.° — *Sia* H *un gruppo transitivo, contenuto in* G, *e permutabile a tutte le sostituzioni di* G. *Siano le lettere di* G *decomponibili in sistemi* Σ, Σ' etc. *tali*; 1° *che solo per ciascuna sostituzione di* H *ciascuno di questi sistemi sia rimpiazzato da un altro*; 2° *che* Σ *contenga un sistema di una delle divisioni*

$$[S, S'...],\ [T, T'...],\ [U, U'...]...[X, X'...]$$

p. e. T, *e sia contenuto in un altro* S. *Essendo* $\frac{k}{\lambda}$ *le lettere di* S *e* $\frac{k}{\lambda\mu}$ *quelle di* T, *le lettere di* Σ *saranno* $\frac{k}{\lambda\mu}$m, *dinotando con* m *un divisore di* μ. *Se si determinano i sistemi* Σ, Σ' etc. *in modo che* m *sia minimo, sarà* μ *una potenza esatta di* m.

Sia h una sostituzione di G non contenuta in H, e siano S ed S' due sistemi di lettere che si scambiano per effetto di questa sostituzione. Indichiamo col simbolo

$$[T_1, T_2...T_m]_{p,q}$$

uno qualunque dei sistemi Σ, Σ' etc. Allora, supponendo che ogni sistema S con-

tenga μ sistemi Σ, potremo rappresentare i sistemi S ed S' coi simboli

$$[(T_1, T_2 \ldots T_m)_{1\cdot 1}\ (T_1, T_2 \ldots T_m)_{1\cdot 2} \ldots (T_1, T_2 \ldots T_m)_{1\cdot \mu}]$$
$$[(T_1, T_2 \ldots T_m)_{2\cdot 1}\ (T_1, T_2 \ldots T_m)_{2\cdot 2} \ldots (T_1, T_2 \ldots T_m)_{2\cdot \mu}].$$

Per la sostituzione h i sistemi T di S debbono scambiarsi con quelli di S'. Supponiamo che le T del sistema $(T_1, T_2 \ldots T_m)_{1\cdot 1}$, appartenente ad S, si scambiino colle T di S' comprese nel simbolo $(T'_1, T'_2 \ldots T'_m)_{2\cdot i}$, per modo che potremo rappresentare S' coll'altro simbolo

$$[(T'_1, T'_2 \ldots T'_m)_{2\cdot 1}\ (T'_1, T'_2 \ldots T'_m)_{2\cdot 2} \ldots (T'_1, T'_2 \ldots T'_m)_{2\cdot \mu}].$$

I complessi $(T'_1, T'_n \ldots T'_m)_{2\cdot i}$, formano dei nuovi sistemi che si scambiano gli uni cogli altri per le sostituzioni del gruppo H trasformato per mezzo di h, ossia dello stesso gruppo H. Di qui segue: 1° che uno dei sistemi $(T'_1, T'_2 \ldots T'_m)_{2\cdot i}$, non possa confondersi con un altro $(T_1, T_2 \ldots T_m)_{2\cdot i}$, perchè altrimenti tutt'i sistemi $(T_1, T_2 \ldots T_m)_{2\cdot i}$, si confonderebbero con tutt'i sistemi $(T'_1, T'_2 \ldots T'_m)_{2\cdot i}$: e quindi per la sostituzione h i sistemi Σ si scambierebbero gli uni cogli altri, il che non è: 2° che due sistemi $(T_1, T_2 \ldots T_m)_{2\cdot i}$, $(T'_1, T'_2 \ldots T_m)_{2\cdot i}$, non possono avere di commune un numero m' di T, minore di m; altrimenti con questi sistemi T si potrebbe formare un altra divisione delle lettere in sistemi che conterrebbero m' sistemi T, il che è contrario alla nostra ipotesi, che m sia minimo. Ma ogni sistema $(T'_1, T'_2 \ldots T'_m)_{2\cdot i}$, deve esser formato da m sistemi T, dunque S' come ogni altro sistema analogo deve contenere m sistemi Σ, epperò conterrà almeno m^2 sistemi Σ.

Se S contiene più di m sistemi Σ, possiamo formare dei nuovi sistemi, riunendo quei sistemi Σ che hanno un sistema T comune con uno degli altri $(T'_1, T'_2 \ldots T'_m)_{2\cdot i}$. Indichiamo col simbolo

(A) $$[(T_1, T_2 \ldots T_m)_{1\cdot 1} \ldots (T_1, T_2 \ldots T_n)_{1\cdot m}]_p$$

uno di questi sistemi. Allora, supponendo che S contenga ν sistemi A, potremo rappresentare S ed $S^{(n)}$ coi simboli

$$[[(T_1, T_2 \ldots T_m)_{1\cdot 1} \ldots (T_1, T_2 \ldots T_m)_{1\cdot m}]_1 \ldots [(T_1, T_2 \ldots T_m)_{1\cdot 1} \ldots (T_1, T_2 \ldots T_m)_{1\cdot m}]_\nu]$$
$$[[(T_1, T_2 \ldots T_m)_{n\cdot 1} \ldots (T_1, T_2 \ldots T_m)_{n\cdot m}]_1 \ldots [(T_1, T_2 \ldots T_m)_{n\cdot 1} \ldots (T_1, T_2 \ldots T_m)_{n\cdot m}]_\nu].$$

Sia g una sostituzione di G per la quale i sistemi A non si scambiino gli uni cogli altri. E supponiamo che per questa sostituzione le lettere di S si scambiino con quelle di $S^{(n)}$. I sistemi T di $S^{(n)}$ si dovranno scambiare coi sistemi T di S; ma i sistemi T di $S^{(n)}$ che si scambiano in corrispondenza coi sistemi T di S si dispongono in sistemi in modo diverso da quello indicato nel simbolo precedente, perciò l'indicheremo coll'altro

$$[[(T_1'', T_2'' \ldots T_m'')_{n\cdot 1} \ldots (T_1'', T_n'' \ldots T_m'')_{n\cdot m}]_1 \ldots [(T_1'', T_2'' \ldots T_m'')_{n\cdot 1} \ldots (T_1'', T_2'' \ldots T_m'')_{n\cdot m}]_\nu].$$

I sistemi

(B) $$B\ [(T_1'', T_2'' \ldots T_m'')_{n\cdot 1} \ldots (T_1'', T_2'' \ldots T_m'')_{n\cdot m}]_i,$$

come anche gli altri $(T_1'', T_2'' \ldots T_m'')_{n\cdot p}$ si scambieranno gli uni cogli altri per le sostituzioni di H trasformate per mezzo di g, ossia per lo sostituzioni di H.

Ora un sistema B non può confondersi con un sistoma A, altrimenti tutt'i sistemi A si confonderebbero con tutt'i sistemi B, e la sostituzione g scambierebbe tra loro i sistemi B, il che non è. Per la stessa ragione un sistema $(T_1, T_2 \ldots T_m)_{n\cdot 1}$, non può confondersi con un sistema $(T_1''. T_2'' \ldots T_m'')_{n\cdot i}$.

Un sistema B non può avere di comune con un sistema A $m' < m$ sistemi T; poichè altrimenti questi sistemi T formerebbero una nuova divisione in sistemi, ciascuno composto di m' sistemi T, il che è contrario all'ipotesi che m sia minimo. Per la stessa ragione i sistemi $(T_1, T_2 \ldots T_m)_{n\cdot i}$, $(T_1'', T_2'' \ldots T_m'')_{n\cdot i}$, non possono avere $m' < m$ sistemi T di comune.

Finalmente B ed A non possono avere di comune le T che formano m' sistemi $(T_1'', T_2'' \ldots T_m'')_{2\cdot i}$, essendo $m' < m$. Poichè se ciò fosse, l'insieme di questi m' sistemi formerebbe un nuovo sistema C, ed allora, appartenendo le T″ di un sistema $(T_1'', T_2'' \ldots T_m'')_{2\cdot i}$, a diversi sistemi $(T_1, T_n \ldots T_m)_{2\cdot i}$, e non contenendo A che m sistemi $(T_1, T_2 \ldots T_m)_{2\cdot i}$, m' sistemi T dovrebbero esser comuni a C ed ad un sistema $(T_1, T_2 \ldots T_m)_{2\cdot i}$; quindi questi sistemi T formerebbero un altro sistema, il che è contrario all'ipotesi che m sia minimo.

Adunque resta, o che le T di un solo sistema $(T_1'', T_2'' \ldots T_m'')_{2\cdot i}$, di B facciano parte di un sistema A, ovvero che le T di un sistema $(T_1'', T_2'' \ldots T_m'')_{2\cdot i}$, appartengano ad m sistemi A. Tanto nell'uno che nell'altro caso $S^{(n)}$ dovrà contenere almeno m sistemi A, e quindi almeno m^3 sistemi T.

Se S contenesse più di m^3 sistemi T, si dimostrerebbe similmente che ne dovrebbe contenere almeno m^4, e così di seguito.

CAPO 7.°

Gruppi composti.

30. Un gruppo dicesi *composto* quando contiene dei gruppi ai quali le sue sostituzioni sono permutabili, e dicesi *semplice* nel caso contrario.

Se G è un gruppo composto, si potrà determinare una serie di gruppi

$$G, H, H', \ldots I, I' \ldots K \ldots, 1, \qquad (1)$$

dei quali l'ultimo sia 1, ed un altro qualunque p. e. H′ sia il più generale di quei gruppi, contenuti nel precedente H, le cui sostituzioni siano permutabili al seguente H″.

Infatti possiamo prima formare la serie dei gruppi

$$G, H, I, K \ldots 1 \qquad (2)$$

dei quali l'ultimo sia 1, ed un altro qualunque p. e. I sia il più generale di quei gruppi, contenuti nel precedente H, a cui le sostituzioni di G siano permutabili. Indi intercalare tra H ed I i gruppi H′, H″... così condizionati: che H′ sia il più generale di quelli contenuti in H e permutabili alle sostituzioni di H, H″ sia il più generale di quelli contenuti in H′ e permutabili alle sue sostituzioni, e così di se-

guito. Nello stesso modo operando sopra ciascuna coppia di gruppi consecutivi della serie (1), si avrà l'altra (2).

Indicando con $N, \frac{N}{\lambda}, \frac{N}{\lambda\mu}, \frac{N}{\lambda\mu\mu'} \ldots\ldots \frac{N}{\lambda\mu\mu'\ldots\nu'}, \frac{N}{\lambda\mu\mu'\ldots\nu\nu'}, \ldots$

gli ordini dei gruppi della serie (1), chiameremo *fattori di composizione* i numeri $\lambda, \mu, \mu' \ldots \nu, \nu \ldots$, e *grado di composizione* di G il loro numero.

40. Teorema 1.° — *Se esiste un' altra serie di gruppi*

$$G, T, T' \ldots\ldots 1 \qquad (3)$$

diversa dalla (1), *ma nello stesso modo condizionata, e sono* $\frac{N}{l}, \frac{N}{lm}, \frac{N}{lmn} \ldots$ *i rispettivi loro ordini, saranno i fattori* l, m, n etc., *prescindendo dall'ordine, identici agli altri* λ, μ, μ' etc.

Supponiamo che nella (1) vi siano soltanto i termini da noi segnati.

Le serie (1) e (3) debbono avere un gruppo comune, almeno l'ultimo. Supponiamo che il 1° gruppo comune sia K. Dinotiamo con a l'ordine di K, e con $1, k_1, k_2 \ldots k_{a-1}$ le sue sostituzioni. Poichè il gruppo K è contenuto in I, il di cui ordine è $a\nu\nu'$, pel teorema di Lagrange, possiamo rappresentare le sue sostituzioni coi simboli

$$\begin{array}{ccccc} 1 & k_1 & k_2 & \ldots\ldots & k_{a-1} \\ i_1 & i_1 k_1 & i_1 k_2 & \ldots\ldots & i_1 k_{a-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ i_{\nu\nu'-1} & i_{\nu\nu'-1} k_1 & i_{\nu\nu'-1} k_2 & \ldots\ldots & i_{\nu\nu'-1} k_{a-1}, \end{array}$$

indicando con i_β delle sostituzioni di I che non soddisfano alle condizioni

$$i_\beta = k_\alpha, \quad i_\beta = i_\beta, k_\alpha.$$

Per modo che, rappresentando col simboli i_0, k_0 l'unità, possiamo indicare le sostituzioni di I col simbolo $i_\beta k_\alpha$, intendendo che β possa variare da zero a $\nu\nu'-1$, ed α da zero ad $a-1$.

Similmente, indicando con $h'_{\gamma'}$ delle sostituzioni di I' che non soddisfano alle condizioni

$$h'_{\gamma'} = i_\beta k_\alpha, \quad h'_{\gamma'} = h'_{\gamma'} i_\beta k_\alpha,$$

possiamo rappresentare le sostituzioni di I' col simbolo $h'_{\gamma'} i_\beta k_\alpha$, potendo γ' variare da 0 a $\mu'-1$. Nello stesso modo, se h_γ e g_δ sono delle sostituzioni di I e di G convenientemente scelte, possiamo rappresentare le sostituzioni di questi gruppi rispettivamente coi simboli $h_\gamma h'_{\gamma'} i_\beta k_\alpha$, $g_\delta h_\gamma h'_{\gamma'} i_\beta k_\alpha$, intendendo che γ possa variare da 0 a $\mu-1$, e δ da 0 a $\lambda-1$.

41. *Il numero delle sostituzioni* di T è $\lambda\mu\mu' a$. Infatti I e T sono contenuti in G, ed I non è contenuto in T; perciò il gruppo L risultante dalla combinazione delle sostituzioni di I e di T sarà contenuto in G e sarà più generale di T, ma le sostituzioni di G, essendo permutabili ad I ed a T, lo sono anche ad L, quindi L deve essere identico a G, altrimenti in G si conterrebbe un gruppo L, più generale di T, a cui le sostituzioni di G sarebbero permutabili, il che è impossibile.

Ora se indichiamo con $S_1, S_2, \ldots S_n$ le sostituzioni di T, quelle di I saranno della forma $i_\beta S_m$. Invero sia $i_\beta k_\alpha S_1 i_{\beta'} k_{\alpha'} S_2$ una di queste sostituzioni. Essa può mettersi sotto la forma $i_\beta k_\alpha i_{\beta'} i_{\beta'}^{-1} S_1 i_{\beta'} k_{\alpha'} S_2$, per essere $i_{\beta'} i_{\beta'}^{-1} = 1$. Ma $i_{\beta'}$, essendo una sostituzione di G, sarà permutabile al gruppo T, e quindi $i_{\beta'}^{-1} S_1 i_{\beta'}$ sarà una sostituzione di T, che indicheremo con S'_1; inoltre la sostituzione $i_\beta k_\alpha i_{\beta'}$, appartenendo ad I, può mettersi sotto la forma $i_{\beta_1} k_{\alpha_1}$, adunque sarà

$$i_\beta k_\alpha S_1 i_{\beta'} k_{\alpha'} S_2 = i_{\beta_1} k_{\alpha_1} S'_1 k_{\alpha'} S_2,$$

e siccome $k_{\alpha'}$, S'_1, k_{α_1}, S_2 sono sostituzioni di T, possiamo porre

$$k_{\alpha_1} S'_1 k_{\alpha_1} S_2 = S_p,$$

quindi sarà $$i_\beta k_\alpha S_1 i_{\beta'} k_{\alpha'} S_2 = i_{\beta_1} S_p.$$

Ma le sostituzioni i_β sono $\nu\nu'$, e l'altre $i_{\beta_1} S_p$ debbono essere quante quelle di G, cioè $\lambda\mu\mu'\nu\nu'a$, dunque le sostituzioni di T debbono essere $\lambda\mu\mu'a$.

42. Le sostituzioni di T fanno parte di G, perciò debbono essere della forma $g_\delta h_\gamma h'_{\gamma'} i_\beta k_\alpha$. *Due di queste sostituzioni, nelle quali δ, γ, γ' hanno gli stessi valori, debbono avere per β valori diversi.* Infatti sia

$$S_1 = g_\delta h_\gamma h'_{\gamma'} i_\beta k_\alpha, \quad S_2 = g_\delta h_\gamma h'_{\gamma'} i_{\beta_1} k_{\alpha_1},$$

sarà $$S_1^{-1} S_2 = (g_\delta h_\gamma h'_{\gamma'} i_\beta k_\alpha)^{-1} g_\delta h_\gamma h'_{\gamma'} i_{\beta_1} k_{\alpha_1},$$

ma $$(g_\delta h_\gamma h'_{\gamma'} i_\beta k_\alpha)^{-1} = (i_\beta k_\alpha)^{-1} (g_\delta h_\gamma h'_{\gamma'})^{-1},$$

quindi sarà $$S_1^{-1} S_2 = (i_\beta k_\alpha)^{-1} (g_\delta h_\gamma h'_{\gamma'})^{-1} (g_\delta h_\gamma h'_{\gamma'})\, i_{\beta_1} k_{\alpha_1} = (i_\beta k_\alpha)^{-1} i_{\beta_1} k_{\alpha_1},$$

ma $$(i_\beta k_\alpha)^{-1} = k_\alpha^{-1}\, i_\beta^{-1},$$

dunque sarà $$S_1^{-1} S_2 = k_\alpha^{-1} i_\beta^{-1} i_{\beta_1} k_{\alpha_1}.$$

Il 2° membro di quest'eguaglianza, essendo il prodotto di più sostituzioni di I, indica una sostituzione di questo gruppo, perciò $S_1^{-1} S_2$ appartiene ad I, ma $S_1^{-1} S_2$ fa anche parte di T, dunque $S_1^{-1} S_2$ sarà una sostituzione comune ad I ed a T. Or se dinotiamo con K' il gruppo formato dalle sostituzioni comuni ad I ed a T, K' dovrà contenere K. Inoltre le trasformate delle sostituzioni di K' per mezzo delle sostituzioni di G debbono essere comuni ad I ed a T, per essere le sostituzioni di G permutabili a questi due gruppi, quindi queste trasformate apparterranno a K', e sarà G permutabile a K'. Di qui risulta che, se K' non si confondesse con K, vi sarebbe un gruppo più generale di K contenuto in I al quale G sarebbe permutabile, il che è contrario alla legge di formazione della serie (1). Dunque le sostituzioni comuni ad I ed a T sono quelle che formano K, epperò sarà

$$S_1^{-1} S_2 = k_\alpha^{-1} i_\beta^{-1} i_{\beta_1} k_{\alpha'} = k_{\alpha_2}$$

donde l'uguaglianza $$i_{\beta_1} = i_\beta\, k_\alpha\, k_{\alpha_2} k_{\alpha'}^{-1} = i_\beta k_{\alpha_3},$$

la quale non può aver luogo se β è diverso da β_1.

43. Dal principio testè dimostrato risulta: che *il simbolo $g_\delta h_\gamma h'_{\gamma'} k_\alpha$ dà una sostituzione di* T *per ogni sistema di valori di γ, δ, γ', α.* Infatti questi sistemi sono $\lambda\mu\mu'a$, quante sono le sostituzioni di T. e ciascuno di essi non può dare che

una sola sostituzione di T, poichè, se ne desse più d'una, queste dovrebbero differire per l'indice β, il che si è dimostrato impossibile.

44. Or siano

$$h'_0 i_{\beta_0} = (h'_0),\quad h'_1 i_{\beta_1} = (h'_1),\quad h'_2 i_{\beta_2} = (h'_2) \ldots h'_{\gamma'} i_{\beta_{\gamma'}} = (h'_\gamma)$$

le sostituzioni di T corrispondenti ai valori $\delta = 0$, $\gamma = 0$, $\alpha = 0$;

$$h_0 i_{\beta'_0} = (h_0)\,,\quad h_1 i_{\beta'_1} = (h_1)\,,\quad h_2 i_{\beta'_2} = h_2 \ldots h_\gamma i_{\beta''_\gamma} = (h_\gamma)$$

quelle corrispondenti ai valori $\delta = 0$, $\gamma' = 0$, $\alpha = 0$;

$$g_0 i_{\beta''_0} = (g_0)\,,\quad g_1 i_{\beta''_1} = (g_1)\,,\quad g_2 i_{\beta''_2} = (g_2) \ldots g_\delta i_{\beta''_\delta} = (g_\delta)$$

quelle corrispondenti ai valori $\gamma = 0$, $\gamma' = 0$, $\alpha = 0$.

Le sostituzioni della forma $(g_\delta)(h_\gamma)(h'_{\gamma'})k_\alpha$ fanno parte di T. Reciprocamente ogni sostituzione di T deve essere di questa forma, perchè essa dà $\lambda\mu\mu'\alpha$ sostituzioni distinte. Infatti se si avesse

$$(g_{\delta_0})(h_{\gamma_0})(h'_{\gamma'_0})k_{\alpha_1} = (g_{\delta_1})(h_{\gamma_1})(h'_{\gamma'_1})k_{\alpha_2}\,,$$

rimettendo in luogo di (g_{δ_0}), (g_{δ_1}), (h_{γ_0}), $(h_{\gamma'_0})$ etc. i rispettivi valori, si avrebbe

$$g_{\delta_0}\mathrm{M} = g_{\delta_1}\mathrm{M}_1$$

donde

$$g_{\delta_0}\mathrm{M}\mathrm{M}_1^{-1} = g_{\delta_1}\,,$$

indicando con M ed M_1 delle sostituzioni di H, derivate da sostituzioni h, h', i, k, appartenenti a questo gruppo. Ma la precedente uguaglianza non può aver luogo che nel solo caso di $\delta_1 = \delta_0$, per essere le g_δ così determinate, che la relazione

$$g_{\delta_1} = g_{\delta_0} \times (\text{sost. H})$$

si verifica solo quando $\delta_1 = \delta_0$, (sost. H) $= 1$, quindi sarà

$$(h_{\gamma_0})(h'_{\gamma'_0})k_{\alpha_1} = (h_{\gamma_1})(h'_{\gamma'_1})k_{\alpha_2}.$$

Similmente si dimostrerebbe che debba essere $\gamma_0 = \gamma_1$, $\gamma'_0 = \gamma'_1$, $\alpha_1 = \alpha_2$.

Parimente le sostituzioni di G, H, H' sono rispettivamente rappresentate dai simboli

$$i_\beta (g_\delta)(h_\gamma)(h'_{\gamma'})k_\alpha\,,\quad i_\beta (h_\gamma)(h'_{\gamma'})k_\alpha\,,\quad i_\beta (h'_{\gamma'})k_\alpha.$$

Poichè ciascuno di questi simboli dà, per tutt' i sistemi di valori che possono assumere gl' indici, delle sostituzioni del gruppo corrispondente, le quali si dimostrerebbero diverse con un ragionamento analogo al precedente; inoltre questi sistemi di valori sono tanti quante sono le sostituzioni del gruppo corrispondente.

Siccome le sostituzioni prima dinotate da g_δ, h_γ, h'_γ sono sparite dal calcolo, possiamo togliere le parentesi che distinguevano le sostituzioni rappresentate da (g_δ), (h_γ), $(h'_{\gamma'})$.

45. Cade qui in acconcio il dimostrare: che *tra una sostituzione* $\mathrm{S} = i_\beta k_\alpha$ di I *ed un altra* $\mathrm{T} = g_\delta h_\gamma h'_\gamma k_\alpha$ di T *esiste la relazione* $\mathrm{ST} = \mathrm{TS}k_{\alpha'}$.

Infatti la sostituzione $\mathrm{S}^{-1}\mathrm{T}^{-1}\mathrm{ST}$ si può considerare come il prodotto delle due sostituzioni $\mathrm{S}^{-1}\mathrm{T}^{-1}\mathrm{S}$ e T. Ora S, essendo contenuta in I, apparterrà a G, e quindi

sarà permutabile a T, ma T^{-1} è una sostituzione di T, dunque $S^{-1}T^{-1}S$ apparterrà anche a T, ma T è sostituzione di T, dunque $S^{-1}T^{-1}ST$ sarà contenuta in T. Inoltre possiamo riguardare $S^{-1}T^{-1}ST$ come il prodotto di S^{-1} per $T^{-1}ST$. Ora T appartiene a T, e quindi a G, perciò T è permutabile ad I, ma S è una sostituzione di I, dunque $T^{-1}ST$ appartiene ad I, ma anche S^{-1} appartiene ad I, dunque $S^{-1}T^{-1}ST$ è una sostituzione di I, ma le sostituzioni comuni ad I ed a T sono quelle che formano K, dunque sarà

$$S^{-1}T^{-1}ST = k_{\alpha_1}, \quad \text{donde} \quad ST = TSk_{\alpha_1}.$$

46. Mediante questa relazione possiamo facilmente dimostrare: che *nella serie* G, H, H′, I, I′...K...1 *non vi possa essere alcun gruppo* I′ *intermedio ad* I *ed a* K. Infatti, se vi fosse, esso sarebbe permutabile alle sostituzioni di I, per ipotesi. Inoltre sarebbe anche permutabile alle sostituzioni della forma $g_\delta h_\gamma h'_{\gamma'}$; invero le sostituzioni di I′ sono della forma $i_\beta k_\alpha$, e la trasformata T_1 di $i_\beta k_\alpha$ per mezzo di $g_\delta h_\gamma h'_{\gamma'}$ può mettersi sotto la forma

$$T_1 = i_\beta k_\alpha (i_\beta k_\alpha)^{-1} (g_\delta h_\gamma h'_{\gamma'})^{-1} i_\beta k_\alpha g_\delta h_\gamma h'_{\gamma'},$$

ma, essendo $i_\beta k_\alpha$ una sostituzione di I e $g_\delta h_\gamma h'_{\gamma'}$ una sostituzione di T, sarà (44)

$$i_\beta k_\alpha g_\delta h_\gamma h'_{\gamma'} = g_\delta h_\gamma h'_{\gamma'} i_\beta k_\alpha k_{\alpha_1},$$

dunque T_1 si può mettere sotto la forma

$$T_1 = i_\beta k_\alpha (i_\beta k_\alpha)^{-1} (g_\delta h_\gamma h'_{\gamma'})^{-1} (g_\delta h_\gamma h'_{\gamma'}) i_\beta k_\alpha k_{\alpha_1},$$

ma $$(g_\delta h_\gamma h'_{\gamma'})^{-1} (g_\delta h_\gamma h'_{\gamma'}) = 1, \quad (i_\beta k_\alpha)^{-1} (i_\beta k_\alpha) = 1,$$

quindi sarà $$T_1 = i_\beta k_\alpha k_{\alpha_1};$$

perciò T_1 apparterrà al gruppo I′, il quale contiene $i_\beta k_\alpha$ e tutte le sostituzioni di K, ma, combinando le sostituzioni della forma $g_\delta h_\gamma h'_{\gamma'}$ con l'altre i_β e k_α, appartenenti ad I, si ottengono tutte le sostituzioni di G, che sono della forma $g_\delta h_\gamma h'_{\gamma'} k_\alpha$, adunque le sostituzioni di G sarebbero permutabili ad I′; e quindi I conterrebbe un gruppo più generale di K, al quale le sostituzioni di G sarebbero permutabili, il che è contrario alla legge di formazione della serie (2).

Or poichè ν dinota il rapporto dell'ordine di I a quello del seguente I′, e νν′ il rapporto dell'ordine di I a quello di K; essendosi dimostrato che K sia il gruppo che immediatamente segue I, νν′ si riduce a ν.

47. Dai principii testè stabiliti possiamo dedurre la dimostrazione del teorema enunciato.

Le sostituzioni $h'_{\gamma'} k_\alpha$ sono comuni ad H′ ed a T, quindi formano un gruppo. Similmente l'altre $h_\gamma h'_{\gamma'} k_\alpha$ sono comuni ad H ed a T, quindi formano un gruppo. Dinotiamo con

$$G, \ T, \ J, \ J', \ K \ldots\ldots 1 \qquad (1)$$

i gruppi formati rispettivamente dalle sostituzioni delle forme

$$i_\beta g_\delta h_\gamma h'_{\gamma'} k_\alpha, \ g_\delta h_\gamma h'_{\gamma'} k_\alpha, \ h_\gamma h'_{\gamma'} k_\alpha, \ h'_{\gamma'} k_\alpha, \ k_\alpha \ldots$$

Gli ordini di questi gruppi sono rispettivamente

$$N,\ \frac{N}{\gamma},\ \frac{N}{\nu\lambda},\ \frac{N}{\nu\lambda\mu},\ \frac{N}{\nu\lambda_1\mu'},\ \ldots;$$

per modo che i fattori di composizione di G, dati dalla serie (3), sono identici, eccetto nell'ordine, a quelli dati dalla (1). Ora dico che la (3) è formata colle medesime leggi con cui è formata la (1).

1.° *Uno qualunque dei gruppi della* (3), *per esempio* J' *è permutabile alle sostituzioni del precedente* J. Infatti le sostituzioni di J risultano da quelle di J' e dall'altre h_γ. Ora J' è permutabile alle sue sostituzioni. L'altre h_γ, facendo parte di H, sono permutabili ad H', ma le sostituzioni di H' sono della forma $i_\beta h'_{\gamma'} k_\alpha$, dunque, per tutt'i valori di β, γ', α, sarà

$$h_\gamma^{-1} i_\beta h'_{\gamma'} k_\alpha h_\gamma = i_{\beta_1} h'_{\gamma_1} k_{\alpha_1},$$

ovvero $$h_\gamma^{-1} i_\beta h_\gamma h_\gamma^{-1} h'_{\gamma'} k_\alpha h_\gamma = i_{\beta_1} h'_{\gamma_1} k_{\alpha_1},$$

ma si ha la relazione (44) $$i_\beta h_\gamma = h_\gamma i_\beta k_{\alpha_2},$$

dunque sarà $$i_\beta k_{\alpha_2} h_\gamma^{-1} h'_{\gamma'} k_\alpha h_\gamma = i_{\beta_1} h'_{\gamma_1} k_{\alpha_1}, \qquad (a)$$

donde $$i_{\beta_1} = i_\beta k_{\alpha_2} h_\gamma^{-1} h'_{\gamma'} k_\alpha h_\gamma k_{\alpha_1}^{-1} h'^{-1}_{\gamma_1};$$

ma, essendo $k_{\alpha_2}, h_\gamma^{-1}, h'_{\gamma'}, k_\alpha, h_\gamma, k_{\alpha_1}^{-1}, h'^{-1}_{\gamma_1}$ sostituzioni di J, il loro prodotto formerà una sostituzione del medesimo gruppo, e si potrà porre sotto la forma $h_{\gamma_2} h'_{\gamma_2} k_{\alpha_3}$; quindi la precedente uguaglianza si trasforma nell'altra

$$i_{\beta_1} = i_\beta h_{\gamma_2} h'_{\gamma_2} k_{\alpha_3},$$

la quale non può aver luogo, che nel caso di $\beta_1 = \beta$ e di $h_{\gamma_2} h'_{\gamma_2} k_{\alpha_3} = 1$. Adunque

la (a) si riduce all'altra $$k_{\alpha_2} h_\gamma^{-1} h'_{\gamma'} k_\alpha h_\gamma = h'_{\gamma_1} k_{\alpha_1},$$

donde $$h_\gamma^{-1} h'_{\gamma'} k_\alpha h_\gamma = h'_{\gamma_1} k_{\alpha_1} k_{\alpha_2}^{-1}.$$

Il 2° membro di quest'uguaglianza dinota una sostituzione di J', perchè $h'_{\gamma_1}, k_{\alpha_1}, k_{\alpha_2}^{-1}$ sostituzioni di questo gruppo. ed il 1° membro dinota la trasformata di una sostituzione della forma $h'_{\gamma'} k_\alpha$ per mezzo di h_γ, dunque questa trasformata appartiene ad J', ma le sostituzioni di questo gruppo sono tutte della forma $h'_{\gamma'} k_\alpha$, dunque h_γ è permutabile ad J', e quindi J' è permutabile alle sostituzioni di J.

2.° *Non esiste alcun gruppo più generale di* J', *contenuto in* J *e permutabile alle sue sostituzioni.*

Supponiamo che esista un tale gruppo J'', ed indichiamo con $S_1, S_2 \ldots S_n$ le sue sostituzioni. Formiamo un gruppo Π colle sostituzioni i_β e coll'altre S_n. Questo gruppo sarà più generale di H'. Infatti le sostituzioni di H', sono della forma $i_\beta h'_{\gamma'} k_\alpha$; ma una sostituzione S_i di Π, che non fa parte di J' è della forma $h_\gamma h'_{\gamma'} k_\alpha$, dunque S_i non appartiene ad H', ma Π contiene tutte le sostituzioni della forma $i_\beta h'_{\gamma'} k_\alpha$, dunque Π è più generale di H'.

Inoltre Π è contenuto in H, ma non si confonde con esso. Infatti, essendo le sostituzioni di H della forma $i_\beta h_\gamma h'_{\gamma'} k_\alpha$, H contiene le sostituzioni i_β e l'altre $h_\gamma h'_{\gamma'} k_\alpha$,

ma di quest'ultime fanno parte le S_n, quindi H contiene le sostituzioni che risultano combinando le i_β con le S_n, ossia contiene Π. Ma se $h_\gamma h'_\gamma k_\alpha$ è una sostituzione di J, non contenuta in J′, essa fa parte di H e non di Π. Infatti questa sostituzione non è della forma S_n, e non può risultare dalla combinazione delle i_β colle S_n; poichè se fosse

$$h_\gamma h'_{\gamma'} k_\alpha = i_\beta S_n i_{\beta'} S_{n'},$$

essendo (44)

$$S_n i_{\beta'} = i_{\beta'} S_n k_{\alpha'},$$

sarebbe

$$i_\beta S_n i_{\beta'} S_{n'} = i_\beta i_{\beta'} S_n k_{\alpha'} S_{n'},$$

ma $i_\beta i_{\beta'}$ è una sostituzione di J, quindi si può porre sotto la forma $i_{\beta_1} k_{\alpha_1}$, epperò sarebbe

$$i_\beta S_n i_{\beta'} = i_{\beta_1} k_{\alpha_1} S_n k_{\alpha'} S_{n'};$$

ma, essendo k_{α_1}, S_n, $k_{\alpha'}$, $S_{n'}$ sostituzioni di J, si può porre

$$k_{\alpha_1} S_n h_{\alpha'} S_{n'} = h_{\gamma_1} h'_{\gamma'_1} k_{\alpha_1},$$

quindi sarebbe

$$i_\beta S_n i_{\beta'} S_{n'} = i_{\beta_1} h_{\gamma_1} h'_{\gamma'_1} k_{\alpha_1},$$

donde l'uguaglianza

$$h_\gamma h'_{\gamma'} k_\alpha = i_\beta h_{\gamma_1} h'_{\gamma'_1} k_{\alpha_1}$$

la quale è impossibile.

Infine Π è permutabile a tutte le sostituzioni di G. Infatti sia $i_\beta T$ una sostituzione di H, essendo T una sostituziono di J, sia inoltro $i_\beta S_n$ una sostituziono di Π. Per essere S_n e T^{-1} sostituzioni di T ed $i_\beta, i_{\beta_1}^{-1} i_\beta i_{\beta_1}$ sostituzioni di I, si hanno le relazioni

$$S_n i_\beta = i_\beta S_n k_\alpha, \quad T^{-1} i_{\beta}^{-1} i_\beta i_{\beta_1} = i_{\beta_1}^{-1} i_\beta i_{\beta_1} T^{-1} k_{\alpha_1};$$

quindi la trasformata $(i_{\beta_1} T)^{-1} i_\beta S_n i_{\beta_1} T$ di $i_\beta S_n$ si può porre sotto la forma

$$i_{\beta_1}^{-1} i_\beta i_{\beta_1} T^{-1} k_{\alpha_1} S_n k_\alpha T = i_{\beta_1}^{-1} i_\beta i_{\beta_1} T^{-1} k_{\alpha_1} T T^{-1} S_n T T^{-1} k_\alpha T.$$

Allora si vede che essa appartiene a Π; infatti Π contiene $i_{\beta_1}^{-1}$, i_β, i_{β_1}, inoltre contieno $T^{-1} S_n T$ che è la trasformata di S_n per mezzo di T, permutabilo ad J″; infine contiene $T^{-1} k_{\alpha_1} T$ e $T^{-1} k_\alpha T$ che sono le trasformate di k_{α_1} e k_α per mezzo di T, permutabile a K.

Adunque se esistesso un gruppo J″ più generale di J′, contenuto in J e permutabile alle sue sostituzioni; vi sarebbe un gruppo Π più generale di H′, contenuto in H, al quale le sostituzioni di H sarebbero permutabili, il che è contrario alla legge di formazione della serie (2).

48. Ora essendo formate le serie

$$G,\ T,\ J,\ J',\ K \ldots\ldots 1 \qquad (4)$$

$$G,\ T,\ T' \ldots\ldots\ldots\ldots 1 \qquad (5)$$

e la (1) colle medesime leggi, saranno altresì in queste condizioni le serie

$$T,\ J,\ J',\ K \ldots\ldots\ldots 1$$

$$T,\ T' \ldots\ldots\ldots\ldots\ldots 1.$$

Ma, essendo l'ordine di T rappresentato tanto da $\frac{N}{l}$ quanto da $\frac{N}{\nu}$, sarà $l = \nu$; quindi, se i fattori di composizione $m, n \ldots$ di T, dati dalla 2ª di queste serie, sono identici, eccetto nell'ordine, ai fattori $\lambda, \mu, \mu' \ldots$ di T, dati dalla 1ª; saranno anche i fattori $l, m, n \ldots$ di G, dati dalla (5), identici ai fattori di G dati dalla (4), e quindi

identici a quelli dati dalla (1). Similmente si dimostrerebbe che se i fattori di T' sono sempre gli stessi, lo saranno anche quelli di T; e così di seguito. Ma questo si verifica pel penultimo gruppo delle (1); perchè esso è semplice: adunque possiamo conchiudere che i fattori di composizione di G siano sempre gli stessi, qualunque sia il modo con cui si è scomposto questo gruppo in altri gruppi parziali, formanti delle serie analoghe alla (1).

Questo teorema mostra che i gruppi composti si possono classificare secondo il numero ed il valore dei fattori di composizione.

49. Teorema 2.° — *Sia* G, H, ... I, K ... 1 *una serie di gruppi, ciascuno dei quali sia il più generale di quelli contenuti nel precedente, e permutabili alle sostituzioni di* G. *Sia* H *un gruppo qualunque di questa serie*, I *e* K *due altri gruppi successivi qualunque. Supponiamo che si possa determinare un gruppo* L *il quale contenga* K, *sia contenuto in* I *e sia permutabile alle sostituzioni di* H: *inoltre supponiamo che, se si possono determinare più di questi gruppi* L, *si scelga quello il cui ordine sia minimo. Allora se* n, mn, μn *sono gli ordini di* K, L, I, *sarà* μ *una potenza di* m.

Se indichiamo con $1, k_1, k_2 \dots k_{n-1}$ le sostituzioni di K, quelle di L possono essere rappresentate dal simbolo $l_\alpha k_\beta$ in cui α varia da 0 ad $m-1$, e β da 0 ad $n-1$, ed l_α è una sostituzione di L che non soddisfa a nessuna delle due condizioni $l_\alpha = k_\beta$, $l_\alpha = l_{\alpha'} k_{\beta'}$.

Poichè L è permutabile alle sole sostituzioni di H, vi dovranno essere in G delle sostituzioni non permutabili ad L; sia g una di queste, ed l'_α la trasformata di l_α per mezzo di g. Allora la trasformata di $l_\alpha k_\beta$ per mezzo di g può essere rappresentata da $l'_\alpha k_{\beta'}$, perchè le sostituzioni di G sono permutabili a K. Ora essendo le sostituzioni di H permutabili ad L, saranno quelle del gruppo $gH^{-1}g$ permutabili al gruppo L', formato dalle sostituzioni $l'_\alpha k_{\beta'}$, ma $gH^{-1}g$ è lo stesso H, dunque le sostituzioni di H sono permutabili ad L', ma le sostituzioni di H sono permutabili ad L, dunque queste medesime sostituzioni sono permutabili al gruppo Δ formato dalle sostituzioni comuni ad L' ed L. Ora queste sostituzioni sono appunto quelle che formano K; poichè, se ve ne fossero anche dell'altre, Δ conterrebbe K, sarebbe contenuto in I, sarebbe permutabile alle sostituzioni di H, ed avrebbe un ordine minore di quello di L, il che è contrario all'ipotesi.

Ora le sostituzioni l_α appartengono ad H, ma g è permutabile ad H, dunque le l'_α fanno parte di H, e perciò sono permutabili ad L. Di qui risulta che si possano mettere sotto la forma $l'_\alpha l_\alpha k_\beta$ le sostituzioni del gruppo Δ', formato dalle derivate da l'_α e dall'altre $l_\alpha k_\beta$ (16).

Due sostituzioni della forma $l'_\alpha l_\alpha k_\beta$ non possono essere uguali. Infatti supponiamo che si avesse

$$l'_{\alpha'} l_\alpha k_\beta = l'_{\alpha'_1} l_{\alpha_1} k_{\beta_1}.$$

Allora sarebbe

$$l'^{-1}_{\alpha'_1} l'_{\alpha'} = l_{\alpha_1} k_{\beta_1} k_\beta^{-1} l_\alpha^{-1},$$

ma il 2° membro di quest'uguaglianza, essendo formato da sostituzioni che appartengono ad L, può porsi sotto la forma $l_{\alpha_2} k_{\beta_2}$; quindi sarebbe

$$l'^{-1}_{\alpha'_1} l'_{\alpha'} = l_{\alpha_2} k_{\beta_2},$$

perciò $l'^{-1}_{\alpha'_1} l'_{\alpha'}$, appartenendo tanto ad L' quanto ad L, farebbe parte di K, laonde sarebbe

$$l'^{-1}_{\alpha'_1} l'_{\alpha'} = k_{\alpha_1},$$

donde

$$l'_{\alpha'} = l'_{\alpha'_1} k_{\alpha_1},$$

e quindi

$$g l'_{\alpha} g^{-1} = g l'_{\alpha'_1} g^{-1} \cdot g k_{\alpha_1} g^{-1},$$

ma

$$g l'_{\alpha} g^{-1} = l_{\alpha'}, \quad g l'_{\alpha'_1} g^{-1} = l_{\alpha'_1}, \quad g k_{\alpha_1} g^{-1} = k_{\alpha_1},$$

quindi sarobbe

$$l_{\alpha'} = l_{\alpha'_1} k_{\alpha_1},$$

il che è vero nel solo caso che $\alpha' = \alpha'_1$, ed allora sarebbe

$$l_{\alpha} k_{\beta} = l_{\alpha_1} k_{\beta_1},$$

e quindi $\alpha = \alpha_1$, $\beta = \beta_1$.

Ma, variando α' e α da 0 ad $m-1$, e β da 0 ad $n-1$, sono $m^2 n$ i sistemi di valori che danno gl'indici della espressione $l'_{\alpha'} l_{\alpha} k_{\beta}$, dunque, essondo contenute in I le sostituzioni $l'_{\alpha'} l_{\alpha} k_{\beta}$, se I si confonde con Δ', I conterrà $m^2 n$ sostituzioni.

Se I contiene anche dell'altre sostituzioni, una di queste, i, può essere la trasformata di un altra sostituzione di I per mezzo di una sostituzione, g', di G; allora, non contenendosi i in Δ', g' non sarà permutabile a Δ'.

Indichiamo con λ_{α}, $\lambda'_{\alpha'}$ le trasformate di l_{α} e di $l'_{\alpha'}$ per mezzo di g', e con Δ'' il gruppo $g'\Delta' g'^{-1}$, il quale sarà permutabile alle sostituzioni di $g'Hg'^{-1}$, ossia alle sostituzioni di H. Ora, essendo H permutabile a Δ' ed a Δ'', lo sarà anche al gruppo formato dalle sostituzioni comuni a Δ' ed a Δ''. Ma Δ'' è distinto da Δ', perciò non può contenere tutte le sostituzioni di L ed L', che insieme combinate danno Δ'. Supponiamo che Δ'' contenga una parte delle sostituzioni di L. Queste non possono essere che quelle che compongono K, altrimenti si potrebbe formare un gruppo che conterrebbe K, sarebbe contenuto in I, sarebbe permutabile alle sostituzioni di H, ed avrebbe un ordine minore di quello di L, il che è contrario all'ipotesi. Di qui risulta che l_{α} sia distinta da $\lambda_{\alpha'}$, da $\lambda'_{\alpha'}$, e da k_{β}.

Ora le sostituzioni $l_{\alpha}\lambda_{\alpha}\lambda'_{\alpha'} k_{\beta}$ sono tutte contenute in I, sono tra loro distinte, e sono $m^3 n$ di numero, dunque I deve contenere $m^3 n$ sostituzioni.

Similmente si dimostrerebbe che, se I contenesse più di $m^3 n$ sostituzioni, ne dovrebbe contenere almeno $m^4 n$, e così di seguito.

CAPO 8.°

Legame delle funzioni coi gruppi.

50. Se $1, \alpha_1, \alpha_2, \ldots \alpha_{m-1}$ sono le sostituzioni di un gruppo G', contenuto in un altro G, le sostituzioni di quest'ultimo possono essere rappresentate da

$$\left.\begin{matrix} 1 & \alpha_1 & \alpha_2 \ldots\ldots \alpha_{m-1} \\ \beta & \alpha_1\beta & \alpha_2\beta \ldots\ldots \alpha_{m-1}\beta \\ \gamma & \alpha_1\gamma & \alpha_2\gamma \ldots\ldots \alpha_{m-1}\gamma \\ \ldots & \ldots & \ldots\ldots\ldots\ldots \end{matrix}\right\} \qquad (1)$$

essendo β, γ etc. delle sostituzioni di G tali, che ciascuna sia diversa dalle sostituzioni contenute nelle linee orizzontali di (1) che precedono quella di cui essa fa parte.

Ora, se una funzione F delle lettere di G non cambia valore per ciascuna delle sostituzioni di G', essa assumerà lo stesso valore per tutte le sostituzioni contenute in una medesima linea orizzontale del quadro (1).

Invero le sostituzioni di una di queste linee, per esempio della 2ª, sono i prodotti delle sostituzioni della 1ª per β; e siccome per le sostituzioni della 1ª linea F non si altera; così i risultati delle sostituzioni della 2.ª linea fatte in F sono identici a quello che si ottiene per la sostituzione β.

Di qui segue che, se m è l'ordine di G' ed n quello di G, sia $\frac{n}{m}$ il numero dei valori distinti che F prende per le sostituzioni di G.

51. *L'insieme di tutte le sostituzioni* 1, m, n... *per le quali una funzione* F *non cambia valore deve formare un gruppo.* Infatti una sostituzione che risulta dal prodotto di due o più delle altre l, m, n... non fa cambiare valore ad F, quindi deve appartenere al precedente complesso.

Il gruppo formato dalle sostituzioni, per cui una funzione non cambia valore, dicesi gruppo della funzione.

52. *Ad ogni gruppo* G *corrisponde una funzione.* Infatti prendiamo la funzione $\varphi = a + 2b + 3c + \ldots$ la quale cambia di valore per ogni sostituzione, ed indichiamo con $\varphi_1, \varphi_2, \varphi_3 \ldots$ i valori che φ prende rispettivamente per le sostituzioni $\alpha, \beta, \gamma \ldots$ di G. La funzione $\varphi_1 \varphi_2 \varphi_3 \ldots$ non cambierà per alcuna sostituzione di G, e cambierà per ogni altra che n'è estranea· poichè, dinotando con σ una sostituzione qualunque di G, il risultato che si ottiene facendo la sostituzione σ in $\varphi_1 \varphi_2 \varphi_3 \ldots$ è identico a quello che si ha, eseguendo in corrispondenza lo sostituzioni $\alpha\sigma, \beta\sigma, \gamma\sigma \ldots$ nei fattori dell'altra $\varphi\varphi\varphi \ldots$, ma quest'ultime sostituzioni sono identiche ad $\alpha, \beta, \gamma \ldots$ prese con ordine diverso, quindi l'esecuzione di σ in $\varphi_1 \varphi_2 \varphi_3 \ldots$ non fa altro che scambiare i fattori, perciò la funzione $\varphi_1 \varphi_2 \varphi_3 \ldots$ non cambierà; ma se σ' è una sostituzione, non contenuta in G, l'altre $\alpha\sigma', \beta\sigma', \gamma\sigma' \ldots$ nemmeno vi saranno contenute, quindi per ciascuna di esse φ deve prendere un valore diverso da $\varphi_1, \varphi_2, \varphi_3$ etc., che perciò per σ cambierà valore la funzione $\varphi_1 \varphi_2 \varphi_3 \ldots$

53. Teorema 1.°— *Se i gruppi di più funzioni* $\varphi, \psi \ldots$ *hanno le stesse sostituzioni* $1, \alpha_1, \alpha_2 \ldots$ *di comune con un gruppo qualunque* G, *una qualunque di esse sarà esprimibile in funzione razionale di un altra delle rimanenti e di funzioni invariabili per le sostituzioni di* G.

Supponiamo che le sostituzioni di G siano quelle indicate nel quadro (1), ed indichiamo con $\varphi_\beta, \psi_\beta$ i risultati che si ottengono facendo la sostituzione β in φ e ψ.

La funzione $$\psi_1 \varphi_1^m + \psi_\beta \varphi_\beta^m + \psi_\gamma \varphi_\gamma^m + \ldots\ldots = t^{(m)} \qquad (2)$$

è invariabile per le sostituzioni di G. Infatti, per una sostituzione σ di G, questa funzione prende la forma

$$\psi_\sigma \varphi_\sigma^m + \psi_{\beta\sigma} \varphi_{\beta\sigma}^m + \psi_{\gamma\sigma} \varphi_{\gamma\sigma}^m + \ldots\ldots = t_\sigma^{(m)} \qquad (3).$$

Ora le sostituzioni $\sigma, \beta\sigma, \gamma\sigma \ldots$ appartengono a G, perciò sono della forma $A\beta, A\gamma, A\delta$ etc. essendo A una delle sostituzioni $1, \alpha_1, \alpha_2 \ldots \alpha_{m-1}$, ma due di esse, per esempio

$\gamma\sigma$ e $\beta\sigma$ non possono essere della medesima forma $A\delta$; poichè, se fosse

$$\beta\sigma = \alpha_1\delta, \quad \gamma\sigma = \alpha_2\delta,$$

sarebbe
$$\delta\sigma^{-1} = \alpha^{-1}\beta = \alpha_2^{-1}\gamma,$$

donde
$$\gamma = \alpha_2\alpha^{-1}\beta = \alpha_i\beta,$$

il che è impossibile, quindi le sostituzioni σ, $\beta\sigma$, $\gamma\sigma$, $\delta\sigma$ ... appartengono a linee diverse del quadro (1); ma per tutte le sostituzioni di una linea orizzontale di questo quadro $\psi\varphi^m$ prende lo stesso valore che assume per la 1ª sostituzione della stessa linea, quindi i termini delle (3), presi con ordine diverso, sono identici a quelli della (2). Supponiamo che le linee orizzontali di (1) siano μ, e facciamo nella (2) successivamente m uguale a 0, 1, 2, ... $\mu - 1$, si avrà

$$\left.\begin{array}{l}
\psi_1 \quad + \psi_\beta \quad + \psi_\gamma \quad + \ldots\ldots = t^{(0)} \\
\psi_1\varphi_1 \quad + \psi_\beta\varphi_\beta \quad + \psi_\gamma\varphi_\gamma \quad + \ldots\ldots = t^{(1)} \\
\psi_1\varphi_1^2 \quad + \psi_\beta\varphi_\beta^2 \quad + \psi_\gamma\varphi_\gamma^2 \quad + \ldots\ldots = t^{(2)} \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\psi_1\varphi_1^{\mu-1} + \psi_\beta\varphi_\beta^{\mu-1} + \psi_\gamma\varphi_\gamma^{\mu-1} + \ldots\ldots = t^{(\mu-1)}.
\end{array}\right\} \qquad (4)$$

Le radici dell'equazione

$$F(x) = (x - \varphi_1)(x - \varphi_\beta)(x - \varphi_\gamma)\ldots = 0$$

sono φ_1, φ_β, φ_γ..., quindi i suoi coefficienti sono funzioni simmetriche di φ_1, φ_β, φ_γ etc. e perciò invariabili per le sostituzioni di G. L'altra equazione

$$f(x) = \frac{F(x)}{x - \varphi_1} = x^{\mu-1} + \lambda_{\mu-1}x^{m-1} + \ldots\ldots + \lambda_0 = 0$$

ha per radici φ_β, φ_γ etc., ed i suoi coefficienti sono funzioni razionali di φ_1 e dei coefficienti di $F(x)$. Ora addizioniamo le (4) dopo averle moltiplicate rispettivamente per λ_0, λ_1 etc., allora i termini che contengono ψ_β, ψ_γ etc. spariscono, e resta

$$\psi_1(\lambda_0 + \lambda_1\varphi_1 + \ldots + \varphi_1^{\mu-1}) = \lambda_0 t^{(0)} + \lambda_1 t^{(1)} + \ldots + t^{(\mu-1)},$$

donde si ricava per ψ_1 il valore

$$\psi_1 = \frac{\lambda_0 t^{(0)} + \lambda_1 t^{(1)} + \ldots + t^{(\mu-1)}}{f(\varphi_1)} = \frac{\lambda_0 t^{(0)} + \lambda_1 t^{(1)} + \ldots + t^{(\mu-1)}}{F'(\varphi_1)}$$

il quale è finito, perchè $F(x) = 0$ ha una sola radice uguale a φ_1.

54. Una funzione di k lettere dicesi alternata quando il gruppo corrispondente è il gruppo alternato di queste lettere, e dicesi simmetrica quando il gruppo corrispondente è quello che contiene tutte le sostituzioni che si possono formare colle k lettere.

55. Teorema 2.° — *Se una funzione F di k lettere a, b, c, ... l, m ... è transitiva e simmetrica o alternata per rispetto a k' lettere a, b, c ..., essendo* $k' > \frac{k}{2}$, *sarà simmetrica o alternata per rispetto a tutte le lettere.*

Il gruppo G di F, essendo transitivo, dovrà contenere una sostituzione S che scambia a con l: supponiamo che la stessa scambiasse $b, c \ldots$ con $x, y \ldots$ Poichè le lettere $a, b, c \ldots$ sono k' e $k' > \frac{k}{2}$, le lettere l, x, y non possono essere tutte contenute nella serie $l, m \ldots$; supponiamo che y non faccia parte di questa serie, e che x sia uguale a c. Poichè F è simmetrica o alternata per rispetto alle lettere $a, b, c \ldots$, G deve contenere tutte le sostituzioni ternarie che si possono formare con queste lettere, perciò conterrà la sostituzione $T = (abc)$ e quindi, l'altra $U = S^{-1}TS = (lcy)$. Inoltre, se α e β sono due lettere qualunque della serie $a, b, c \ldots$, G conterrà le sostituzioni $V = (\alpha\beta c)$, $V^2 = (\alpha c\beta)$, e quindi l'altre $W = V^{-1}UV = (l\alpha y)$, $W' = V^{-2}UV^2 = (l\beta y)$. Ora combinando le tre sostituzioni U, W, W' si ha

$$UW = (lcy)(l\alpha y) = (lc)(ly)(ly)(l\alpha) = (lc)(l\alpha) = (lc\alpha)$$

$$UW' = (lcy)(l\beta y) = (lc)(ly)(ly)(l\beta) = (lc)(l\beta) = (lc\beta)$$

$$WW' = (l\alpha y)(l\beta y) = (l\alpha)(ly)(ly)(l\beta) = (l\alpha)(l\beta) = (l\alpha\beta),$$

ma $(lc\alpha)$, $(lc\beta)$, $(l\alpha\beta)$ sono le tre sostituzioni circolari di 3° ordine che si possono formare con l, α, β, ed α e β sono due lettere qualunque della serie $a, b, c, \ldots$; dunque G contiene tutte le sostituzioni ternarie che si possono formare colle lettere $a, b, c, \ldots l$, le quali costituiscono il gruppo alternato di queste lettere. Ma nel caso che F è simmetrica per rispetto ad $a, b, c \ldots$ G deve contenere tutte le sostituzioni di queste lettere equivalenti ad un numero impari di trasposizioni, e perciò (22. Co. 2°) G deve esser formato da tutte le sostituzioni che si possono ottenere colle lettere $a, b, c \ldots l$; adunque, se F è simmetrica o alternata per rispetto ad $a, b, c \ldots$, lo sarà anche per rispetto ad $a, b, c \ldots l$.

Se y fa anche parte della serie $a, b, c \ldots$, G conterrà le sostituzioni $V = (cy\alpha)$, $V' = (cy\beta)$, quindi l'altre $V^{-1}UV = (ly\alpha)$, $V'^{-1}UV' = (ly\beta)$, ma combinando queste due ultime sostituzioni con U si hanno le tre sostituzioni circolari di 3° ordine $(lc\alpha)$, $(lc\beta)$, $(l\alpha\beta)$, quindi resta ferma la deduzione innanzi fatta.

Ora essendo F simmetrica o alternata per rispetto ad $a, b, c \ldots l$, lo sarà per rispetto ad $a, b, c \ldots l, m$, e così di seguito.

CAPO 9.°

Isomorfismo.

56. Un gruppo H si dice *isomorfo* ad un altro G, quando si verificano le due seguenti condizioni: 1° che ciascuna sostituzione di G corrisponde ad una sola sostituzione di H, e ciascuna sostituzione di H corrisponde ad una o più sostituzioni di G: 2° che il prodotto di due sostituzioni qualunque di G corrisponde al prodotto delle sostituzioni corrispondenti di H. L'isomorfismo dicesi *meriedrico*, quando più sostituzioni di G corrispondono ad una sola sostituzione di H, ed *oloedrico* nel caso contrario.

57. Teorema 1.° — *Se un gruppo H è isomorfo ad un altro G, ed a una sostituzione di H corrispondono m sostituzioni di G, sarà l'ordine di G m volte maggiore di quello di H.*

Siano $g_1, g_2, g_3 \dots g_m$ le m sostituzioni di G corrispondenti alla sostituzione γ di H, inoltre sia g' un altra sostituzione di G e γ' la corrispondente in H. Poichè alla sostituzione 1 di G corrisponde la sostituzione 1 in H; alla sostituzione $g_1 g_1^{-1}$ dovrà corrispondere l'altra $\gamma\gamma'^{-1}$, ma g_1 corrisponde a γ, quindi g_1^{-1} corrisponderà a γ^{-1}. Di qui risulta che le sostituzioni g', $g_2 g_1^{-1} g'$, $g_3 g_1^{-1} g'$, ... $g_m g_1^{-1} g'$ di G corrisponderanno alla sostituzione $\gamma\gamma^{-1}\gamma'$, ossia γ', di H, quindi ad ogni sostituzione di H corrisponderanno m sostituzioni di G.

58. Teorema 2.° — *Le sostituzioni di G corrispondenti alla sostituzione 1 di H formano un gruppo H', permutabile alle sostituzioni di G.*

Siano 1, h_1, h_2, ... h_{m-1} le sostituzioni di H'. Il prodotto di due o più di queste sostituzioni deve corrispondere alla sostituzione 1 di H, perciò formerà parte di H', e quindi H' sarà un gruppo.

Or sia g una sostituzione di G, non compresa in H', e γ la corrispondente in H: la sostituzione $gh_n g^{-1}$ corrisponderà a $\gamma'\gamma^{-1}$, ossia ad 1, quindi $gh_n g^{-1}$ formerà parte di H', epperò H' sarà permutabile alle sostituzioni di G.

Corollario. — Poichè i gruppi composti sono quelli che contengono altri gruppi permutabili alle loro sostituzioni, solo i gruppi composti possono avere dei gruppi isomorfi con meriedria.

59. Teorema 3.° — *I gruppi intransitivi isomorfi ad un dato gruppo G si scindono in altri gruppi transitivi isomorfi a G, ed i gruppi transitivi isomorfi a G si compongono in altri gruppi intransitivi isomorfi a G.*

Sia G' un gruppo intransitivo isomorfo a G. Inoltre siano $a_1, a_2 \dots a_m$ le lettere che le sostituzioni di G scambiano con a; $b_1, b_2, \dots b_n$ quelle che le medesime sostituzioni scambiano con b, e così di seguito. Allora le sostituzioni di G debbono essere della forma AB..., A'B'..., A''B''..., essendo A, A', A''... delle sostituzioni che permutano tra loro le a; B, B', B''... delle sostituzioni che permutano tra loro le b, e così di seguito. Ora i complessi di sostituzioni A, A'...; B, B'...; ... sono dei gruppi transitivi isomorfi a G. Infatti le A, le B etc., permutando lettere diverse, sono tra loro mutabili, quindi il prodotto delle due sostituzioni AB..., A'B'... si può porre sotto la forma AA'...BB'..., ma questa sostituzione, facendo parte di G, può mettersi sotto la forma $A_n B_n$..., quindi sarà $A_n =$ AA'..., $B_n =$ BB'..., etc., ma A_n, B_n etc. fanno rispettivamente parte dei complessi A, A'...; B, B'...; ...: dunque ciascuno di questi complessi contiene il prodotto di due o più sostituzioni che gli appartengono, epperò è un gruppo. Inoltre è transitivo, perchè per le sue sostituzioni una delle sue lettere si può scambiare con ciascuna delle rimanenti. Ma a ciascuna sostituzione di G' corrisponde una sostituzione in ciascuno dei gruppi (A, A'...), (B, B'...), etc., ed al prodotto di due sostituzioni di G' corrisponde il prodotto delle sostituzioni corrispondenti in ciascuno dei precedenti gruppi, dunque sarà ciascuno di essi isomorfo a G', e quindi a G.

Siano $(A, A' \ldots)$, $(B, B' \ldots)$ etc. dei gruppi transitivi isomorfi a G, e permutino rispettivamente le lettere $a, a_1, a_2 \ldots$; $b, b_1, b_2 \ldots$; etc. È chiaro che i prodotti $AB\ldots$; $A'B'\ldots$; etc. i di cui fattori sono le sostituzioni dei gruppi proposti, corrispondenti ad una medesima sostituzione di G, formino un gruppo H'' intransitivo ed isomorfo a G, poichè ogni sostituzione di H'' corrisponde ad una sostituzione di ciascuno dei gruppi proposti, ed al prodotto di due sostituzioni di H'' corrisponde il prodotto delle due corrispondenti in ciascuno dei gruppi proposti.

Corollario. — Di qui risulta, che la ricerca dei gruppi isoformi ad un gruppo dato G si riduca a quella dei gruppi transitivi isomorfi a G.

60. Teorema 4.° — *Ad ogni gruppo contenuto in un altro G corrisponde un gruppo transitivo isomorfo a G.*

Se $1, h_1, h_2 \ldots h_{m-1}$ sono le sostituzioni di un gruppo H, contenuto in G, ed α, β, γ etc. delle sostituzioni di G convenientemente scelte, tutte le sostituzioni di G saranno contenute nel quadro

$$\begin{array}{cccc} 1 & h_1 & h_2 & \ldots\ldots h_{m-1} \\ \alpha & h_1\alpha & h_2\alpha & \ldots\ldots h_{m-1}\alpha \\ \beta & h_1\beta & h_2\beta & \ldots\ldots h_{m-1}\beta \\ \vdots & \vdots & \vdots & \vdots \end{array}$$

Or se F è una funzione delle lettere di G, la quale resta inalterata, operandovi le sostituzioni di G, essa prenderà lo stesso valore per tutte le sostituzioni contenute nella medesima linea orizzontale del quadro precedente: infatti per operare la sostituzione $h_n\alpha$ su di F, bisogna prima operare h_n e poi α, ma per la 1ª F non cambia, dunque si ha per $h_n\alpha$ lo stesso risultato che per α. Laonde se indichiamo con F_α il valore che prende F per una sostituzione qualunque α, i diversi valori, che potrà prendere F per tutte le sostituzioni di G, saranno

$$F, \; F_\alpha, \; F_\beta \ldots\ldots$$

Se sopra le funzioni F, F_α, F_β etc. si opera una sostituzione di G, queste si scambieranno tra loro. Infatti supponiamo che si operi la sostituzione $h_n\alpha$, allora F_γ prenderà il valore che assumerà F operandovi la sostituzione $\gamma h_n\alpha$, ma questa sostituzione, facendo parte di G, sarà contenuta in una linea orizzontale del quadro precedente diversa dalla 2ª e dalla 3ª; supponiamo che faccia parte della 4ª che incomincia con δ, allora darà per risultato F_δ. Di qui risulta che operando le sostituzioni di G sopra i singoli fattori del prodotto $FF_\alpha F_\beta \ldots$ si avrà una serie di permutazioni dello stesso prodotto, e le sostituzioni per cui da questo si passa alle sue permutazioni formeranno evidentemente un gruppo H', il quale sarà transitivo, poichè le sostituzioni di G fanno prendere ad F uno qualunque dei valori F_α, F_β etc. Inoltre è isomorfo a G, perchè ad ogni sostituzione di G corrisponde una sostituzione di questo gruppo, ed al prodotto di due sostituzioni di G corrisponde il prodotto delle sostituzioni corrispondenti del medesimo gruppo.

61. Osservazione. — *Se le sostituzioni di G sono permutabili ad H, a tutte le sostituzioni comprese in una linea orizzontale del quadro precedente corrisponderà una sola sostituzione di H'.*

Infatti, oparando le sostituzioni γ ed $h_n\gamma$ sopra le lettere di G contenute in ciascuno dei fattori del prodotto

$$(a) \qquad F F_\alpha F_\beta \ldots\ldots,$$

si otterranno le due permutazioni

$$(b) \qquad F_\gamma F_{\alpha\gamma} F_{\beta\gamma} \ldots\ldots \qquad\qquad (c) \qquad F_{h_n\gamma} F_{\alpha h_n\gamma} F_{\beta h_n\gamma} \ldots\ldots$$

Ma, per essere le sostituzioni di G permutabili ad H, si ha

$$\alpha h_n = h_{n'}\alpha, \quad \beta h_n = h_{p'}\beta,$$

quindi la (c) si riduce all'altra $F_{h_n\gamma} F_{h_{n'}\alpha\gamma} F_{h_{p'}\beta\gamma} \ldots\ldots$ ovvero all'altra $F_\gamma F_{\alpha\gamma} F_{\beta\gamma} \ldots\ldots$, perchè le sostituzioni h non alterano F, dunque le permutazioni (b) e (c) sono identiche, e perciò sono altresì identiche le sostituzioni di H' che da (a) deducono (b) e (c). Laonde nel caso in parola l'ordine ed il grado di H' sono uguali.

Se le sostituzioni di G non sono permutabili ad H, l'ordine di H' è uguale a quello di G.

62. Teorema 5.° — *Ogni gruppo transitivo isomorfo a G si deduce da uno di quelli contenuti in G nel modo indicato nella dimostrazione del teorema precedente.*

Siano G' un gruppo transitivo ed isomorfo a G, $1, h_1, h_2 \ldots h_{n-1}$ le sostituzioni di G, corrispondenti alla sostituzione 1 di G', ed F una funzione delle lettere x, x_1, x_2 etc. di G che non cambia, operando sulle x le sostituzioni h. Se i valori assunti da F per le sostituzioni di G sono rappresentati da $F, F_1, F_2 \ldots F_{n-1}$, operando le sostituzioni di G sopra $F F_1 F_2 \ldots F_{m-1}$ si avrà una serie di permutazioni di questo prodotto, e le sostituzioni per le quali da una di esse si passa all'altre formeranno un gruppo Γ, il quale sarà isomorfo a G, ed avrà tanto il grado quanto l'ordine uguale al rapporto m dell'ordine di G a quello del gruppo $(1, h_1, h_2 \ldots)$ (58 Co. 61), ma a questo medesimo rapporto è uguale l'ordine di G', dunque Γ sarà isomorfo a G' senza meriedria.

Supponiamo che $y, y_1, y_2 \ldots$ siano le lettere che permutano le sostituzioni di G'. Poniamo

$$F' = \alpha y + \alpha_1 y_1 + \alpha_2 y_2 + \ldots$$

ed intendiamo operate su questa funzione tutte le sostituzioni di G', si avranno così tanti risultati diversi $F', F'_1, F'_2 \ldots F'_{m-1}$ quant'è l'ordine di G'. E se operiamo le sostituzioni di G' sopra il prodotto $F' F'_1 F_2 \ldots F'_{m-1}$ si avrà una serie di permutazioni del medesimo, le quali daranno luogo ad un gruppo Γ' isomorfo senza meriedria a G', e quindi a Γ, ed il suo ordine come il suo grado saranno uguali all'ordine di G'.

I gruppi Γ *e* Γ' *sono identici.*

Infatti il gruppo Γ è transitivo; perciò il suo ordine deve essere uguale al suo grado moltiplicato pel numero di sostituzioni che lasciano immobile una data lettera, ma l'ordine ed il grado sono uguali ad m, dunque una sola sostituzione di Γ lascia immobile una data lettera, ed è la sostituzione 1; di qui risulta che Γ non può contenere due sostituzioni che scambiano una lettera x con un'altra x_1,

poichè, moltiplicando l'una per l'inversa dell'altra, si avrebbe una sostituzione, diversa dall'unità, che lascierebbe immobile una lettera, il che è impossibile. Quello che si è detto di Γ è applicabile a Γ'.

Or sia F_n quella delle funzioni $F, F_1, F_2 \ldots$ che la sostituzione γ_n di Γ fa succedere ad F, e sia F'_n quella delle funzioni $F', F'_1, F'_2 \ldots$ che la sostituzione γ'_n di Γ', corrispondente a γ_n, fa succedere ad F'. Se la sostituzione δ di Γ scambia F_p con F_q, la corrispondente δ' di Γ' scambierà F'_p con F'_q. Infatti la sostituzione $\gamma_p^{-1}\gamma_q$ fa succedere F_q ad F_p, ma questa sola sostituzione di Γ può far succedere questo scambio, dunque $\delta = \gamma_p^{-1}\gamma_q$, ma il prodotto di due sostituzioni di Γ deve corrispondere al prodotto delle corrispondenti di Γ', dunque $\delta' = \gamma'_p{}^{-1}\gamma'_q$, donde si ha che δ' scambierà F'_p con F'_q.

Di qui risulta che se (F_p, F_q, F_r) è un ciclo di δ, (F'_p, F'_q, F'_r) dovrà essere un ciclo di δ', quindi le due sostituzioni saranno identiche, e per conseguenza saranno anche identici i gruppi Γ e Γ'.

Supponiamo che fosse

$$\left.\begin{aligned} F' &= \alpha y + \alpha_1 y_1 + \alpha_2 y_2 + \ldots \\ F'_1 &= \alpha_1 y + \alpha y_1 + \alpha_2 y_2 + \ldots \\ F'_2 &= \alpha_2 y + \alpha_1 y_1 + \alpha y_2 + \ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}\right\} \quad (1)$$

Poichè $\alpha, \alpha_1, \alpha_2 \ldots$ sono costanti arbitrarie, possiamo mediante le precedenti equazioni esprimere linearmente y, y_1 etc. in funzione di F', F'_1 etc. Supponiamo che si avesse

$$\left.\begin{aligned} y &= \beta F' + \beta_1 F'_1 + \beta_2 F'_2 + \ldots \\ y_1 &= \beta_1 F' + \beta F'_1 + \beta_2 F'_2 + \ldots \\ y_2 &= \beta_2 F' + \beta_1 F'_1 + \beta F'_2 + \ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}\right\} \quad (2)$$

Or se si operano sulle y delle (1) le sostituzioni di G', i primi membri di quest'uguaglianze si scambieranno nello stesso modo che questi si scambiano per le sostituzioni di Γ'. E se si operano le sostituzioni di Γ' nelle (2), i primi membri si scambieranno come viene indicato dalle sostituzioni di G'. Quindi, se dinotiamo con $z, z_1, z_2 \ldots$ le funzioni composte colle F nel medesimo modo che le y sono composte colle F', operando sulle F le sostituzioni di Γ, le quali sono identiche a quelle di Γ', si debbono avere sulle z le stesse sostituzioni di G'. Ma le sostituzioni di Γ, fatte sulle F, equivalgono alle sostituzioni di G fatte sulle lettere x contenute nelle F, dunque le sostituzioni di G' sono identiche alle sostituzioni che si ottengono tra le z, z_1, z_2 etc. se sulle x contenute in queste funzioni si operano le sostituzioni di G. Ma il numero delle z, z_1, z_2 etc. è minore dell'ordine di G, perchè esse sono tante quante sono le y, y_1, y_2 etc., dunque G dovrà contenere più sostituzioni che, operate sulle x di z, danno lo stesso risultato, ma ciascuna di queste sostituzioni deve essere il prodotto di due sostituzioni, l'una delle quali non altera z, quindi G dovrà contenere più sostituzioni che non altereranno z, le quali formeranno un gruppo.

Da quanto è stato detto si raccoglie: 1° che z sia una funzione delle x, x_1 etc. che non si altera per le sostituzioni di un gruppo contenuto in G: 2° che z, z_1, z_2 etc. siano i diversi valori che prende z quando sulle x si operano tutte le sostituzioni di G: 3° che operando le sostituzioni di G sulle x di ciascuno dei fattori z del prodotto $z z_1 z_2$ etc. si ottengano altre permutazioni di questo prodotto le quali si possano avere da $z z_1 z_2$ etc., operando sulle z di questo prodotto delle sostituzioni identiche alle sostituzioni tra le y che compongono G'.

63. Teorema 6.° — *Due gruppi isomorfi senza meriedria sono nello stesso tempo semplici o composti, e se sono composti i fattori di composizione dell'uno sono uguali a quelli dell'altro,*

Siano G e G' i due gruppi, e supponiamo che G contenga il gruppo H, formato dalle sostituzioni 1, h_1, h_2... In G' vi saranno le sostituzioni corrispondenti a quelle che formano H ed il prodotto di due qualunque di esse, quindi esse formeranno un gruppo H' dello stesso ordine di H, perchè ad ogni sostituzione di G corrisponde una sola sostituzione di G'. Ora se le sostituzioni di G sono permutabili ad H, dinotando con g e g' due sostituzioni corrispondenti di G e G', e con h'_n, $h'_{n'}$ le sostituzioni di H' che corrispondono alle sostituzioni h_n, $h_{n'}$ di H, si avrà

$$g h_n g^{-1} = h_{n'}, \quad g' h'_n g'^{-1} = h'_{n'},$$

quindi le sostituzioni di G' sono permutabili ad H'. Di qui segue che se con G, supposto gruppo composto, si forma la serie di gruppi

G, L, K 1

tali che ciascuno sia il più generale di quelli contenuti nel precedente e permutabili al seguente, con G' si potrà formare una serie analoga di gruppi

G', L', K' 1;

e gl'ordini dei gruppi della 1ª serie saranno uguali agl'ordini dei gruppi corrispondenti della 2ª, perciò i fattori di composizione di G saranno uguali a quelli di G'.

CAPO 10.°

Limite in meno del numero dei valori che può prendere una funzione, permutando le sue lettere.

64. Teorema 1.° — *Una funzione F di k lettere simmetrica o alternata per rispetto a k — n di esse avrà meno valori di un'altra funzione F' di k lettere la quale non gode di questa proprietà.*

Questa proposizione cadrà talora in difetto per i piccoli valori di k. ma si potrà sempre assegnare a k un limite al di là del quale essa sarà vera.

In questa dimostrazione si suppone che k sia un numero grandissimo.

Il numero dei valori, che prende una funzione di k lettere, per effetto delle permutazioni di queste lettere, si ottiene dividendo il numero delle permutazioni che si possono formare con k lettere per l'ordine del gruppo G di questa funzione.

Ma, essendo F simmetrica o alternata per rispetto a $k-n$ delle sue lettere, G deve contenere il gruppo alternato di queste lettere, il di cui ordine è $\frac{1\cdot 2\cdot 3\ldots(k-n)}{2}$; quindi l'ordine di G è divisibile per questo numero, laonde il numero dei valori di F è un divisore di

$$2k(k-1)(k-2)\ldots\ldots(k-n+1).$$

65. Supponiamo che F' sia intransitiva, ossia che il suo gruppo G' sia intransitivo. Allora le sue lettere si possono dividere in sistemi tali, che ciascuna sostituzione di G' permuti tra loro le lettere di uno stesso sistema. E se indichiamo con $\alpha, \alpha_1, \alpha_2$ etc. i numeri delle lettere che compongono questi diversi sistemi, l'ordine di G' è un divisore di

$$1\cdot 2\cdot 3\ldots\alpha\cdot 1\cdot 2\cdot 3\ldots\alpha_1\cdot 1\cdot 2\cdot 3\ldots\alpha_2\ldots,$$

quindi il numero dei valori che può prendere F' è un multiplo di

$$\frac{1\cdot 2\cdot 3\ldots k}{1\cdot 2\cdot 3\ldots\alpha\cdot 1\cdot 2\cdot 3\ldots\alpha_1\cdot 1\cdot 2\cdot 3\ldots\alpha_2\ldots}.$$

Dovendo essere la somma $\alpha+\alpha_1+$ etc. uguale a k, saranno k i fattori del denominatore della precedente espressione, ed i loro valori aumenteranno, crescendo α e diminuendo il numero ed i valori di α_1, α_2 etc. Quindi se F' è transitivo per rispetto ad un numero di lettere minore di $k-n$, il minimo numero degli altri α_1, α_2 etc. è 1, il minimo valore, che può prendere α_1, è $n-1$, ed il massimo valore, che può prendere α, è $k-n+1$. Laonde il minimo valore che può prendere la precedente frazione è

$$\frac{1\cdot 2\cdot 3\ldots k}{1\cdot 2\cdot 3\ldots(k-n-1)\cdot 1\cdot 2\cdot 3\ldots(n+1)}$$

ovvero
$$\frac{k(k-1)\ldots(k-n)}{1\cdot 2\cdot 3\ldots(n+1)};$$

e questo è il minimo numero di valori che può assumere F'. Laonde il numero dei valori di F' sarà maggiore del numero dei valori di F, se

$$\frac{k(k-1)\ldots(k-n)}{1\cdot 2\cdot 3\ldots(n+1)} > 2k(k-1)\ldots(k-n+1)$$

donde
$$k-n > 2\cdot 1\cdot 2\cdot 3\ldots(n+1).$$

66. Or supponiamo che F' sia transitiva per rispetto alle $k-\nu$ lettere a, b, c etc., essendo ν un numero che può variare da zero ad n. In questo caso le sostituzioni di G' debbono essere della forma AB, A'B' etc., essendo A, A' etc. delle sostituzioni sulle lettere a, b, c etc., e B, B' etc. delle sostituzioni che permutano le rimanenti ν lettere.

Il gruppo (A, A'...) non può contenere il gruppo alternato delle lettere a, b, c etc., che chiameremo H. Infatti l'ordine di H è $\frac{1\cdot 2\cdot 3\ldots(k-\nu)}{2}$, e quello del gruppo (B, B'...) è al più $1\cdot 2\cdot 3\ldots\nu$, ma il 1° di questi due numeri è grandissimo per rispetto al 2°,

per essere k grandissimo per rispetto ad n, e quindi per rispetto a $\nu < n$, adunque, dovendo le sostituzioni di G' risultare dalla combinazione delle A colle B, dovrà G' contenere almeno due sostituzioni AB, $A'B'$ nelle quali $B=B'$, ed A, A' sono due sostituzioni distinte di H. Perciò G' conterrà $AB(A'B')^{-1}=AA'^{-1}$, tutte le trasformate di AA'^{-1} per mezzo di AB, $A'B'$ etc., e tutte le derivate da queste trasformate. Ma le trasformate di AA'^{-1} per mezzo di AB, $A'B'$ etc. equivalgono alle trasformate di AA'^{-1} per mezzo di A, A' etc., quindi G' conterrà le trasformate di AA'^{-1} per mezzo di tutte le sostituzioni di H, nonchè le loro derivate, e per conseguenza il gruppo H', formato da tutte queste sostituzioni, sarà comune a G' ed ad H, essendo evidente che sia contenuto in H.

Ora le sostituzioni di H sono permutabili ad H'. Infatti la trasformata di $A''AA'^{-1}A''^{-1}$ per mezzo di A''' è $A'''A''AA'^{-1}A''^{-1}A'''^{-1}$, ma

$$A''^{-1}A'''^{-1}=(A'''A'')^{-1},$$

quindi questa trasformata può mettersi sotto la forma $A'''A''AA'^{-1}(A'''A'')^{-1}$, ma $A'''A''$ è una sostituzione di H, quindi le sostituzioni di H sono permutabili a quelle delle sostituzioni di H' che sono delle trasformate di AA'^{-1}, per conseguenza H è permutabile anche alle derivate da queste trasformate, perchè la trasformata di un prodotto è uguale al prodotto delle trasformate dei fattori. Ma H (32. Co.), non può contenere un gruppo al quale le sue sostituzioni sono permutabili, quindi H' coincide con H, e perciò F' sarebbe alternata per rispetto ad a, b, c etc., il che è contrario all'ipotesi.

Ciò premesso, se indichiamo con M l'ordine del gruppo $(A, A' \ldots)$, sarà M il numero dei sistemi di posizioni che possono assumere le lettere a, b, c etc. per le sostituzioni di G', ma le sostituzioni di G' che non spostano queste lettere sono al più $1\cdot2\cdot3\ldots\nu$, dunque (29) l'ordine di G' sarà al più uguale ad $1\cdot2\cdot3\ldots\nu M$, e per conseguenza il numero N dei valori di F' sarà almeno uguale ad

$$\frac{1\cdot2\cdot3\ldots(k-\nu)}{M}\cdot\frac{(k-\nu+1)\ldots k}{1\cdot2\cdot3\ldots\nu}.$$

La frazione $\frac{1\cdot2\cdot3\ldots(k-\nu)}{M}$ rappresenta il numero dei valori che può prendere una funzione transitiva F_1 di $k-\nu$ lettere, la quale non è simmetrica, nè alternata; quindi, dinotando con $\varphi(k-\nu)$ questo numero, sarà N almeno uguale a

$$\frac{(k-\nu+1)\ldots k}{1\cdot2\cdot3\ldots\nu}\varphi(k-\nu),$$

e quindi sarà maggiore del numero dei valori che può prendere F, se

$$\frac{(k-\nu+1)\ldots k}{1\cdot2\cdot3\ldots\nu}\varphi(k-\nu) > 2k(k-1)\ldots(k-n+1),$$

ossia
$$\varphi(k-\nu) > 1\cdot2\cdot3\ldots\nu\cdot2(k-\nu)\ldots(k-n+1)$$

67. Cerchiamo ora un limite inferiore del numero $\varphi(k-\nu)$. Supponiamo che F_1 sia μ volte transitiva. Allora le sostituzioni del suo gruppo G'' debbono spostare più di $2\mu-4$ lettere, quindi tutte le sostituzioni di $2\mu-4$ lettere non fanno parte di G''; da ciò segue che, operando queste tali sostituzioni sopra F_1, non si

potranno avere risultati identici ad F_1, ne' due di questi risultati potranno essere identici tra loro, poichè se le sostituzioni L ed L' di $2\mu-4$ lettere dessero risultati identici, il prodotto LL'^{-1} non cambierebbe F_1, e quindi dovrebbe far parte del gruppo di F_1, il che non è. Laonde F_1 avrà almeno $1\cdot2\cdot3\ldots(2\mu-4)$ valori. Or questo numero sarà maggiore dell'altro

$$1\cdot2\cdot3\ldots\nu\cdot2\,(k-\nu)\ldots(k-n+1),$$

se μ è grandissimo, e tale che sia finito il rapporto di k a μ, poichè allora $(\nu+1)\ldots(\mu-2)$ sarà maggiore di $(k-\nu)\ldots(k-n+1)$, contenendo il 1° di questi prodotti $n-\nu$ fattori infinitamente grandi, ed il 2° $\mu-\nu-2$ fattori simili.

Ma se μ è piccolissimo per rispetto a k, ragioniamo nel seguente modo. Poichè F_1 è μ volte transitiva, l'ordine del suo gruppo G'' è uguale a $(k-\nu)\ldots(k-\mu-\nu)M'$, indicando con M' l'ordine del gruppo intransitivo formato da quelle sostituzioni di G'', che lasciano immobili μ lettere e spostano le rimanenti $k-\mu-\nu$ (29). Quest'ultime si dividono in sistemi tali, che per ciascuna sostituzione di G'' si permutano tra loro le lettere di ciascun sistema, (28) e, se α, α_1, α_2 etc. sono i numeri di lettere dalle quali sono formati questi sistemi, M' è un divisore del prodotto $1\cdot2\cdot3\ldots\alpha\cdot1\cdot2\cdot3\ldots\alpha_1\ldots$ (28. Co. 2°), quindi $\varphi(k-\nu)$ è un multiplo di

$$\frac{1\cdot2\cdot3\ldots(k-\mu-\nu)}{1\cdot2\cdot3\ldots\alpha\cdot1\cdot2\cdot3\ldots\alpha_1\cdot1\cdot2\cdot3\ldots\alpha_2\ldots}.$$

Or supponiamo che α sia il più grande dei numeri $\alpha, \alpha_1\,\alpha$ etc. e che $\alpha_1+\alpha_2+\ldots>n-\nu$; allora si ha il minimo valore, che può assumere l'espressione precedente, quando si pone

$$\alpha=k-\mu-\nu-(n-\nu+1)=k-\mu-n-1,\quad \alpha_1=n-\nu+1,\quad \alpha_2=0,\quad \alpha_3=0\ldots,$$

perciò esso è $\quad\dfrac{(k-\mu-\nu)\ldots(k-\mu-n)}{1\cdot2\ldots(n-\nu+1)}.$

Questa quantità è evidentemente maggiore dell'altra

$$1\cdot2\cdot3\ldots\nu\cdot2\,(k-\nu)\ldots(k-n+1);$$

poichè, se si moltiplicano entrambe per $1\cdot2\cdot3\ldots(n-\nu+1)$, si ottengono l'altre due

$$(k-\mu-\nu)\ldots(k-\mu-n),\quad 1\cdot2\cdot3\ldots(n-\nu+1)\cdot1\cdot2\ldots\nu\cdot2\,(k-\nu)\ldots(k-n+1),$$

la 1ª delle quali contiene $n-\nu+1$ fattori infinitamente grandi, e la 2ª $n-\nu$ fattori simili.

Ma se $\alpha_1+\alpha_2\ldots \overset{=}{<} n-\nu$, cercheremo di porre sotto altra forma il valore

$$\frac{1\cdot2\cdot3\ldots(k-\mu-\nu)}{M'}$$

di $\varphi(k-\nu)$. Perciò osserviamo che le sostituzioni di G'' sono della forma A_1B_1, $A'_1B'_1$ etc.; essendo A_1, A'_1 etc. delle sostituzioni sulle α lettere del 1° sistema, e B_1, B'_1 etc. delle sostituzioni sulle rimanenti $k-\mu-\nu-\alpha$. Ora il numero dei sistemi diversi di posizioni che le sostituzioni di G'' possono dare alle α lettere del 1° sistema è quanto l'ordine del gruppo $(A_1, A'_1\ldots)$, che indicheremo con M''.

Inoltre le sostituzioni che non spostano le lettere del 1° sistema, generalmente, permutano tra loro tutte le lettere di ciascuno dei rimanenti sistemi, perciò l'or-

dine del gruppo formato da quest' ultime sostituzioni deve essere un divisore del prodotto $1\cdot2\cdot3\ldots\alpha_1\times1\cdot2\cdot3\ldots\alpha_2\times\ldots$, quindi M' è uguale ad M'' moltiplicato per questo divisore, per conseguenza, ponendo

$$k'=k-\nu-\mu-\alpha_1-\alpha_2\ldots,$$

$\varphi(k-\nu)$ sarà un multiplo di

$$\frac{(k-\nu-\mu)\ldots(k'+1)}{1\cdot2\ldots\alpha_1\cdot1\cdot2\ldots\alpha_2\ldots}\times\frac{k'(k'-1)\ldots2\cdot1}{M''}.$$

Ora il gruppo $(A_1A'_1\ldots)$ non può contenere il gruppo alternato delle α lettere del 1° sistema, che chiameremo H''. Infatti, se A_1, A'_1 etc. sono le sostituzioni di H'', le corrispondenti di G'' saranno A_1B_1, $A'_1B'_1$ etc., ma il numero $\frac{k'(k'-1)\ldots2\cdot1}{2}$ delle sostituzioni A_1 di H'' è grandissimo per rispetto a quello delle sostituzioni B_1, che al più è $1\cdot2\ldots\alpha_1\cdot1\cdot2\ldots\alpha_2\ldots$, dunque G'' dovrà contenere almeno due sostituzioni A_1B_1, $A'_1B'_1$ nelle quali $B_1=B'_1$, e quindi conterrà $A_1B_1(A'_1B'_1)^{-1}=A_1A'^{-1}_1$, tutte le trasformate di $A_1A'^{-1}_1$ per mezzo di A_1B_1, $A'_1B'_1$ etc., ossia per mezzo di A_1, A'_1 etc., o tutte le derivate da queste trasformate. Ma il gruppo, formato da queste trasformate e dalle loro derivate, essendo contenuto in H'' ed essendo permutabile alle sue sostituzioni deve esser identico ad H''. Dunque G'' conterrà H'', e per conseguenza F_1 sarà simmetrica o alternata per rispetto a k' lettere, ma F_1 è transitiva, e k' è maggiore di $\frac{k-\nu}{2}$; dunque F_1 sarà simmetrica o alternata (56), il che non è.

Quindi l'espressione $$\frac{k'(k'-1)\ldots2\cdot1}{M''}$$

dinota il numero dei valori che può prendere una funzione transitiva di k' lettere F_2, la quale non è simmetrica, nè alternata.

68. Supponiamo che F_2 sia μ volte transitiva, allora il minimo numero dei valori che può prendere è $1\cdot2\cdot3\ldots(2\mu'-1)$, dunque $\varphi(k-\nu)$ sarà almeno uguale a questo prodotto; ma, se μ' è grandissimo in modo che il rapporto di k a μ' è finito, il prodotto $1\cdot2\cdot3\ldots(2\mu'-h)$ è maggiore di $1\cdot2\ldots\nu\cdot2(k-\nu)\ldots(k-n+1)$, dunque in questo caso sarà

$$\varphi(k-\nu)>1\cdot2\ldots\nu\cdot2(k-\nu)-(k-n+1).$$

Ma se μ' è piccolissimo per rispetto a k, possiamo porre M'' sotto la forma $k'(k'-1)\ldots(k'-\mu'+1)M'''$, essendo M''' l'ordine del gruppo intransitivo G''', formato dalle sostituzioni di G'' che lasciano immobili μ' lettere e permutano le rimanenti $k'-\mu'$. Queste lettere si dividono in sistemi tali, che ciascuna sostituzione di G''' permuta tra loro le lettere di ciascun sistema. E, se indichiamo con α', α'_1, $\alpha'_2\ldots$ i numeri di lettere che compongono questi sistemi, M''' sarà un divisore di $1\cdot2\ldots\alpha'\cdot1\cdot2\ldots\alpha'_1\ldots$, per modo che $\varphi(k-\nu)$ sarà un multiplo di

$$\frac{(k-\nu-\mu)\ldots(k'+1)}{1\cdot2\ldots\alpha_1\cdot1\cdot2\ldots\alpha_2\ldots}\times\frac{(k'-\mu')\ldots2\cdot1}{1\cdot2\ldots\alpha'\cdot1\cdot2\ldots\alpha'_1\ldots}.$$

Se $\alpha'_1+\alpha'_2+\ldots>n-\nu-\alpha_1-\alpha_2\ldots$, si avrà il minimo valore di quest'espressione,

ponendo $\alpha' = k' - \mu' - n - \nu - \alpha_1 - \alpha_2 \ldots - 1$, $\alpha'_1 = n - \nu - \alpha_1 - \alpha_2 \ldots + 1$, $\alpha'_2 = \alpha'_3 = \ldots = 0$ e si otterrà

$$\frac{(k-\nu-\mu)\ldots(k'+1)}{1\cdot 2\ldots\alpha_1\cdot 1\cdot 2\ldots\alpha_2\ldots}\times\frac{(k'-\mu')\ldots(k'-\mu'-n-\nu+\alpha_1+\alpha_2+\ldots)}{1\cdot 2\cdot 3\ldots(n-\nu-\alpha_1-\alpha_2\ldots+1)}.$$

Questa quantità è maggiore di $1\cdot 2\ldots\nu\cdot 2(k-\nu)\ldots(k-n+1)$, poichè moltiplicando l'una e l'altra per

$$1\cdot 2\ldots\alpha_1\cdot 1\cdot 2\ldots\alpha_2\ldots 1\cdot 2\ldots(n-\nu-\alpha_1\ldots+1)$$

si avranno due prodotti, dei quali il 1° conterrà $n-\nu+1$ fattori grandissimi, ed il 2° $n-\nu$ fattori simili.

Ma, se $\alpha'_1+\alpha'_2+\ldots \underset{<}{=} n-\nu-\alpha_1-\alpha_2\ldots$, osserviamo che M''' è un divisore di $1\cdot 2\ldots\alpha'_1\cdot 1\cdot 2\ldots\alpha'_2\ldots M^{IV}$, essendo M^{IV} l'ordine del gruppo G^{IV} formato dalle permutazioni delle α' lettere del 1° sistema, prodotte dalle sostituzioni di G''', quindi $\varphi(k-\nu)$ sarà un multiplo di

$$\frac{(k-\nu-\mu)\ldots(k'+1)}{1\cdot 2\ldots\alpha_1\cdot 1\cdot 2\ldots\alpha_2\ldots}\times\frac{(k'-\mu')\ldots(k''+1)}{1\cdot 2\ldots\alpha'_1\cdot 1\cdot 2\ldots\alpha'_2\ldots}\times\frac{k''(k''-1)\ldots 1}{M^{IV}}$$

essendo $$k''=k'-\mu'-\alpha'_1-\alpha'_2\ldots$$

69. Ora si esamina: 1° il caso se l'ordine di transitività di G^{IV}, μ'', è paragonabile a K: 2° se essendo μ'' piccolissimo rispetto a K, dividendo le $k''-\mu''$ lettere in sistemi di α'', α''_1, α''_2 etc. lettere, è $\alpha''_1 > n-\nu-\alpha_1-\alpha_2\ldots-\alpha'_1-\alpha'_2\ldots$ ovvero $\alpha'' \underset{<}{=} n-\nu-\alpha_1-\alpha_2\ldots\alpha'_1-\alpha'_2\ldots$ Seguitando a ragionare in questo modo, si giungerà a dimostrare il teorema in tutt'i casi; poichè, essendo i numeri

$$\alpha_1+\alpha_2+\ldots,\quad \alpha'_1+\alpha'_2+\ldots,\ldots$$

almeno uguali ad 1, gli altri

$$n-\nu,\quad n-\nu-\alpha_1-\alpha_2\ldots,\quad n-\nu-\alpha_1-\alpha_2\ldots-\alpha'_1-\alpha'_2\ldots$$

saranno decrescenti, quindi, se questi secondi fossero costantemente minori dei primi, vi sarebbe un'infinità di numeri minori di $n-\nu$, il che è impossibile.

70. Trovando il limite in meno di k al di là del quale si verifica il teorema dimostrato, quando si suppone che F sia simmetrica o alternata per rispetto a $k-1$ lettere, si dimostrano i tre seguenti teoremi, dovuti a Bertrand.

1.° *Ogni funzione di* k *lettere ha almeno* k *valori distinti*, se essa *non* è *simmetrica, nè alternata.*

2.° *Ogni funzione di* k *lettere, che ha* k *valori distinti, è simmetrica rispetto a* k − 1 *lettere.*

3.° *Una funzione di* k *lettere, che ha più di* k *valori, ne ha almeno* 2k, se k > 7.

Il 1° teorema presenta la seguente eccezione. Se $k=4$, le funzioni il di cui gruppo deriva dalle sostituzioni (ab), (cd), $(ac)(bd)$, come sarebbe $ab+cd$, non sono simmetriche, nè alternate, ed hanno tre valori distinti.

Il 3° teorema presenta la seguente eccezione. Se $k=6$, le funzioni il di cui gruppo deriva dalle due sostituzioni $(abcd)$, $(becd)(cdef)$, come la seguente

$$(ab+cd+ef)\,(ac+bc+fd)\,(ad+bf+ce)\,(ae+bd+fc)\,(af+bc+ed),$$

non simmetriche rispetto a cinque lettere, hanno sei valori distinti.

71. Ciò premesso procediamo alla ricerca dell'indicato limite di k. Se una funzione F di k lettere è intransitiva, le sue lettere si possono dividere in sistemi tali, che ogni sostituzione del suo gruppo H permuti tra loro le lettere di ciascun sistema: e se questi sistemi si compongono rispettivamente di α, α_1, α_2 etc. lettere, l'ordine di H è un divisore di $1\cdot2\ldots\alpha\cdot1\cdot2\ldots\alpha_1\cdot1\cdot2\ldots\alpha_2\ldots$, quindi il numero dei valori di F è un multiplo di $\frac{1\cdot2\cdot3\ldots k}{1\cdot2\ldots\alpha\cdot1\cdot2\ldots\alpha_1\ldots}$. Ora il minimo valore, che può assumere quest'espressione, è k, e si ottiene ponendo $\alpha=k-1$, $\alpha_1=1$, $\alpha_2=\alpha_3=\ldots=0$. In questo caso F è simmetrica per rispetto a $k-1$ lettere. Se si pone $\alpha=\frac{k-1}{2}$, $\alpha_1=1$, $\alpha_2=\alpha_3=\ldots=0$, si ottiene il valore $2k$ che corrisponde al caso in cui F è alternata per rispetto a $k-1$ lettere. Infine se si suppone $\alpha=k-2$, $\alpha_1=2$, $\alpha_2=\alpha_3=\ldots0$, si ottiene il valore $\frac{k(k-1)}{2}$, che è maggiore di $2k$, quando $k>5$.

Se la funzione F è μ volte transitiva, l'ordine del suo gruppo H è uguale a $k(k-1)\ldots(k-\mu+1)M$, essendo M l'ordine di un gruppo intransitivo G, formato dalle sostituzioni di H che lasciano immobili μ lettere. Supponiamo che le lettere permutate da G si dividano nei sistemi

$$a, a_1, a_2\ldots;\quad b, b_1, b_2\ldots;\ldots$$

composti rispettivamente di α, α_1, etc. lettere, e tali che ogni sostituzione di G permuti tra loro le lettere di ciascun sistema. Allora $1\cdot2\ldots\alpha\cdot1\cdot2\ldots\alpha_1\ldots$ è l'ordine del gruppo I, derivato dalle sostituzioni che si possono formare colle lettere di ciascun sistema. Inoltre supponiamo che α sia il più grande dei numeri α, α_1, $\alpha_2\ldots$; ed indichiamo con β il più piccolo dei due numeri α e μ, e con G' il gruppo formato da tutte le sostituzioni che si possono avere con β lettere del 1° sistema a, a_1, a_2 etc. I gruppi G e G' sono contenuti in I, e l'ordine di G' è $1\cdot2\cdot3\ldots\beta$. Ma G' non contiene alcuna sostituzione simile a qualcuna di quelle che compongono G, perchè tutte le sostituzioni di G spostano più di β lettere (30), quindi l'ordine di I è divisibile pel prodotto degli ordini di G e di G' (18. Co.), perciò M è un multiplo di $\frac{1\cdot2\ldots\alpha\cdot1\cdot2\ldots\alpha'_1\ldots}{1\cdot2\ldots\beta}$, e per conseguenza il numero dei valori di F è un multiplo di

$$\frac{1\cdot2\cdot3\ldots(k-\mu)}{1\cdot2\ldots\alpha\cdot1\cdot2\ldots\alpha_1\ldots}\,1\cdot2\ldots\beta.$$

72. Or facciamo diverse ipotesi sopra i valori di α, α_1 etc.

1.° Se $\alpha=\alpha_1=\ldots=1$, il minimo numero di valori che può assumere F è $1\cdot2\cdot3\ldots(k-\mu)$. E poichè μ non può superare $\frac{k}{2}$ (31. Co. 2°), questo numero di valori è maggiore di $2k$, se $k>7$; è anche maggiore di $2k$, se $k=6$, purchè non si abbia $\mu=3$, il che costituisce il caso di eccezione testè notato; infine è maggiore di k, se $k=5$.

2.° Se $\alpha = 2$, gli altri numeri α_1, α_2 etc. possono essere uguali ad 1 o a 2 ed il quozientc ρ di $k - \mu$ per 2 indica quanti al più dei numeri α, α_1, α_2 etc. possono essere uguali a 2; quindi in questo caso il numero dei valori di F è almeno uguale ad $\frac{1 \cdot 2 \ldots k - \mu}{2^\rho} 1 \cdot 2 \ldots \beta$. Or se si sopprimono ρ fattori 2 dal numeratore della frazione, restano i fattori impari, e quindi vi è il 3, supponendo $k < 7$, ma nel caso di $\mu=1$, la precedente espressione si riduce ad $\frac{1 \cdot 2 \ldots (k-1)}{2^\rho}$, quindi dopo la soppressione dei fattori 2 resta al numeratore uno dei fattori $k-1$, $k-2$, perciò la suddetta espressione è almeno uguale ad uno dei due numeri $3(k-2)$, $3(k-1)$ che sono maggiori di $2k$. Se $\mu > 1$ il numero dei valori di F è $\frac{1 \cdot 2 \ldots (k-\mu)}{2^{\rho-1}}$ almeno, ma dopo la soppressione di $\rho - 1$ fattori 2 dal numeratore di questa frazione restano i fattori 3 e $k - \mu$; quindi questo tale numero è almeno uguale a $3(k-2)$, se $\mu = 2$, ed a $3(k-3)$ se $\mu = 3$, ed è evidente che i numeri $3(k-2)$, $3(k-3)$ sono maggiori di $2k$. Ma se $\mu > 3$, osserviamo che il numero dei valori di F non può essere minore di $1 \cdot 2 \cdot 3 \ldots \mu$, quindi, se μ è tale che questo prodotto risulta minore di $2k$, sarà $3\mu < k$, e quindi $3(k-\mu) > 2k$. In fine se $k \overset{=}{<} 7$, ma maggiore di 4, uno dei limiti

$$\frac{1 \cdot 2 \cdot 3 \ldots (k-\mu)}{2^\rho} 1 \cdot 2 \ldots \beta, \; 1 \cdot 2 \ldots \mu$$

risulta maggiore di k

Fa eccezione al ragionamento innanzi fatto il caso di $k=6$ e $\mu=3$. Ma allora le α debbono essere tutte uguali ad 1, perchè altrimenti vi sarebbero nel gruppo di F delle sostituzioni che sposterebbero meno di 4 lettere, il che è impossibile per un gruppo tre volte transitivo.

3.° Se $\alpha > 2$ ed uguale a $k - \mu - 1$ e $\mu < 3$; il numero dei valori di F è $\frac{1 \cdot 2 \ldots (k - \mu - 1)}{N}(k-\mu)$, essendo N l'ordine del gruppo formato dalle sostituzioni di H che permutano le lettere a, a_1, a_2 etc. Or questo gruppo non può contenere il gruppo alternato di a, a_1, a_2, etc., ossia F non può essere simmetrica o alternata per rispetto a queste lettere. Infatti se consideriamo F come funzione delle $k - \mu + 1$ lettere $a, a_1, \ldots d, e$, essa è semplicemente transitiva; perchè $\mu - 1$ lettere restano fisse, e perciò una sola delle lettere $a, a_1, \ldots d$, e può occupare un posto qualunque. Intanto se F fosse simmetrica o alternata per rispetto ad a, a_1, etc., sarebbe anche simmetrica o alternata per rispetto ad $a, a_1, \ldots d, e$ (55), e quindi più d'una volta transitiva per rispetto a queste lettere. Adunque N è uguale o minore di $\frac{1 \cdot 2 \ldots (k - \mu - 1)}{3}$ (25), donde

$$\frac{1 \cdot 2 \ldots (k - \mu - 1)}{N} \overset{=}{<} 3,$$

ed il numero dei valori di F è almeno uguale a $3(k-\mu)$, che sempre supera k, ed anche $2k$ se $k < 7$.

4.° Se $\alpha > 2$ e minore di $k-\mu-1$, e $\mu < 3$, il numero dei valori di F è un multiplo di

$$\frac{1\cdot 2\cdot 3\ldots(k-\mu)}{1\cdot 2\ldots\alpha\cdot 1\cdot 2\ldots\alpha_1\ldots}\,1\cdot 2\ldots\beta,$$

e quindi almeno uguale a $\dfrac{(k-\mu-1)(k-\mu)}{2}\,1\cdot 2\ldots\beta,$

che è sempre maggiore di k, e di $2k$ se $k > 7$.

5.° Se $\alpha > 2$, $\mu > 2$, e quindi $\beta > 2$; il numero dei valori di F è almeno uguale a $(k-\mu)1\cdot 2\ldots\beta$, che è sempre maggiore di $2k$. Poichè la frazione $\dfrac{1\cdot 2\ldots(k-\mu)}{1\cdot 2\ldots\alpha\cdot 1\cdot 2\ldots\alpha_1\ldots}$, rappresentando il numero dei valori di una funzione intransitiva di $k-\mu$ lettere, è almeno uguale a $k-\mu$.

Nel ragionamento che si è fatto si è escluso il caso di $k=4$, poichè in questo caso come nell'altro di $k<4$ si potrebbe costruire il quadro dei diversi gruppi possibili, e così si vedrebbe: che il 1° teorema è vero, come anche il 2°, eccettuando per $k=4$ il caso innanzi notato.

73. La ricerca del limite di k, quando F è simmetrica o alternata per rispetto a $k-2$ lettere, ci conduce alla dimostrazione del seguente:

Teorema 2.° — *Ogni funzione* I *che non è simmetrica nè alternata per rispetto a* $k-2$ *lettere ha più di* $k(k-1)$ *valori.*

Supponiamo che il gruppo G di I sia intransitivo, e che le sue lettere si dividano nei sistemi

$$a, a_1, a_2\ldots;\quad b, b_1, b_2\ldots;\ldots$$

composti rispettivamente di α, α_1, α_2 etc. lettere, e tali che ogni sostituzione di G permuti tra loro le lettere di ciascun sistema, allora le sostituzioni di G saranno della forma AB, A'B' etc.; essendo A, A' etc. delle sostituzioni che permutano le lettere del 1° sistema, e B, B' etc. delle sostituzioni che permutano le lettere rimanenti.

Ora se il più grande dei numeri α, α_1, α_2 etc., che supporremo essere α, è uguale o maggiore di $k-2$, il gruppo (A, A'...) non può contenere il gruppo alternato H delle lettere a, a_1 etc. Infatti l'ordine di H è almeno uguale ad $\dfrac{1\cdot 2\cdot 3\ldots(k-2)}{2}$ e quello del gruppo (B, B'...) è al più $1\cdot 2$, quindi tra le sostituzioni AB, A'B' etc. vi debbono essere necessarismente due sostituzioni AB, A'B' nelle quali A ed A' sono due sostituzioni distinte di H, e B=B', quindi G dovrebbe contenere $AB(A'B')^{-1}=AA'^{-1}$, tutte le trasformate di AA'^{-1} per mezzo di AB, A'B' etc., e le loro derivate; ma, siccome in AA'^{-1} si contengono le sole lettere a, a_1 etc., le trasformate di AA'^{-1} per mezzo di AB, A'B' etc., sono appunto le trasformate di AA'^{-1} per mezzo delle sostitnzioni di H, quindi G conterrebbe il gruppo formato dalle trasformate di AA'^{-1} per mezzo delle sostituzioni di H, e dalle loro derivate; ma questo gruppo, essendo contenuto in H ed essendo permutabile alle sue sostituzioni, deve coincidere con H, dunque G conterrebbe H, ed I sarebbe simmetrica o alternata per rispetto a $k-2$ lettere, il che è contrario all'ipotesi.

Or poichè il gruppo $(A, A'...)$ è transitivo ed il suo grado è maggiore di 7, perchè esso è almeno uguale a $k-2$ e $k>12$, il numero dei valori della funzione di cui $(A, A'...)$ è il gruppo sarà maggiore di 2α, ma questo numero si ottiene, dividendo il prodotto $1\cdot 2 \ldots \alpha$ per l'ordine di $(A, A'...)$; quindi, se s'indica con M quest'ordine, sarà

$$\frac{1\cdot 2\cdot 3 \ldots \alpha}{M} > 2\alpha,$$

donde

$$M < \frac{1\cdot 2\cdot 3 \ldots \alpha}{2\alpha}.$$

Ciò premesso osserviamo che, essendo l'ordine di G uguale ad M moltiplicato per un divisore del prodotto $1\cdot 2 \ldots \alpha \cdot 1\cdot 2 \ldots \sigma_1 \ldots$, il numero N dei valori di I sarà un multiplo di $\frac{1\cdot 2 \ldots k}{M\cdot 1\cdot 2 \ldots \alpha \cdot 1\cdot 2\cdot \alpha_1 \ldots}$, ma il massimo valore che può prendere il prodotto $1\cdot 2 \ldots \alpha \cdot 1\cdot 2 \ldots \alpha_1 \ldots$ è $1\cdot 2$, nel caso di $\alpha = k-2$, ed è 1 quando $\alpha > k-2$; dunque N sarà almeno uguale ad $\frac{1\cdot 2 \ldots k}{1\cdot 2\cdot M}$ nel 1° caso, ed ad $\frac{1\cdot 2 \ldots k}{M}$ nel secondo; e, sostituendo in luogo di M il suo limite, sarà nel 1° caso

$$N > k(k-1)(k-2),$$

e nel 2°

$$N > 2k(k-1),$$

quindi sarà sempre

$$N > k(k-1).$$

Se $\alpha < k-2$, il minimo valore di $\frac{1\cdot 2\cdot 3 \ldots k}{1\cdot 2 \ldots \alpha \cdot 1\cdot 2 \ldots \alpha_1 \ldots}$ sarà $\frac{k(k-1)(k-2)}{1\cdot 2\cdot 3}$, e quindi $N > k(k-1)$.

Supponiamo che I sia μ volte transitiva. In questo caso ogni sostituzione di G deve spostare più di $2\mu-4$ lettere (31), quindi tutte le sostituzioni che si possono formare con $2\mu-4$ lettere debbono far variare I, e due di esse non possono dare per I risultati identici, per conseguenza I avrà almeno $1\cdot 2\cdot 3 \ldots (2\mu-4)$ valori. Ora se $\mu \geqq \frac{k}{4}-2$, essendo $k>12$, dovrà essere μ almeno uguale a 5, e quindi l'ultimo fattore del prodotto $1\cdot 2\cdot 3 \ldots (2\mu-4)$ sarà almeno uguale a 6, e perciò esso conterrà i fattori 3 e 4, distinti dai due ultimi, ma nel caso più svantaggioso questi due ultimi fattori sono $k-5$, $k-8$ i quali, moltiplicati rispettivamente per 4 e per 3, danno i prodotti $4k-36$ e $3k-24$ che sono maggiori di k, dunque nel caso più svantaggioso il prodotto $1\cdot 2\cdot 3 \ldots (2\mu-4)$ sarà maggiore di k^2, e con più ragione maggiore di $k(k-1)$.

Sia $\mu < \frac{k}{2}-2$. Il numero N dei valori che può prendere I è un multiplo di

$$\frac{1\cdot 2\cdot 3 \ldots (k-\mu)}{1\cdot 2 \ldots \alpha \cdot 1\cdot 2 \ldots \alpha_1 \ldots}\, 1\cdot 2 \ldots \beta;$$

supponendo: 1° che le lettere permutate dalle sostituzioni di G, che non spostano μ lettere date, si possano dividere in sistemi composti di α, α_1, α_2 etc. lettere, e tali che ciascuna delle indicate sostituzioni permuti tra loro le lettere di ciascun sistema: 2° che β indichi il più piccolo dei due numeri α e μ, essendo α il più grande

dei numeri α, α_1, α_2 etc. se $\alpha < k-\mu-2$, il minimo valore della precedente espressione è

$$\frac{(k-\mu-2)\,(k-\mu-1)\,(k-\mu)}{1\cdot 2\cdot 3},$$

il quale è maggiore di $k\,(k-1)$ anche nel caso più svantaggioso di $\mu = \frac{k}{2} - 3$.

Se $\alpha \overset{=}{>} k-\mu-2$, osserviamo che le sostituzioni di G le quali permutano unicamente le lettere dei sistemi testè indicati sono della forma A_1B_1, $A'_1B'_1$ etc. essendo A_1, A'_1 etc. delle sostituzioni che permutano le lettere del sistema formato da α lettere, e B_1, B'_1 etc. delle sostituzioni che permutano le lettere dei rimanenti sistemi. Ora il gruppo $(A_1A'_1\ldots)$ non può essere simmetrico, nè alternato, poichè altrimenti I sarebbe alternato o simmetrico per rispetto ad α lettere, ma $\alpha > \frac{k}{2}$, quindi I sarebbe simmetrico o alternato, il che è contrario alla nostra ipotesi. Ma α è maggiore di 7, dunque il numero dei valori che può prendere la funzione, il di cui gruppo è $(A_1A'_1)$, sarà maggiore di 2α, ossia sarà $\frac{1\cdot 2\cdot 3\ldots\alpha}{M} > 2\alpha$, indicando con M l'ordine del gruppo $(A_1A_1'\ldots)$.

Or se β è il più piccolo dei due numeri α e μ, il numero N dei valori di I è un multiplo di

$$\frac{1\cdot 2\cdot 3\ldots(k-\mu)}{M\cdot 1\cdot 2\ldots\alpha_1\cdot 1\cdot 2\ldots\alpha_2\ldots}\,1\cdot 2\ldots\beta;$$

ma nel nostro caso $\mu < \alpha$, donde $\beta = \mu$, quindi N è un multiplo di

$$\frac{1\cdot 2\cdot 3\ldots(k-\mu)}{M\cdot 1\cdot 2\ldots\alpha_1\cdot 1\cdot 2\ldots\alpha_2\ldots}\,1\cdot 2\ldots\mu;$$

ma se $\alpha = k-\mu-2$, il prodotto $1\cdot 2\ldots\alpha_1\cdot 1\cdot 2\ldots\alpha_2\ldots$ è uguale ad $1\cdot 2$, ed è $k-\mu-1 > 1\cdot 2$, dunque N non può essere minore di

$$\frac{1\cdot 2\ldots(k-\mu-2)}{M}\,(k-\mu)\cdot 1\cdot 2\ldots\mu;$$

e se $\alpha = k-\mu-1$, il prodotto $1\cdot 2\ldots\alpha_1\cdot 1\cdot 2\ldots\alpha_2\ldots$ si riduce ad 1, e quindi N non può essere minore di

$$\frac{1\cdot 2\cdot 3\ldots(k-\mu-1)}{M}\,(k-\mu)\cdot 1\cdot 2\ldots\mu.$$

Adunque, tanto se $\alpha = k-\mu-2$ quanto se $\alpha > k-\mu-2$, N non può esser minore di

$$\frac{1\cdot 2\cdot 3\ldots\alpha}{M}\,(k-\mu)\cdot 1\cdot 2\ldots\mu,$$

e perciò non può essere minore di

$$2\alpha\,(k-\mu)\cdot 1\cdot 2\cdot 3\ldots\mu;$$

ma crescendo μ, il suddetto prodotto cresce finchè $k > 2\mu + 1$, quindi N non può essere minore di $2\alpha\,(k-1)$, ma 2α, anche quando $\alpha = k-\mu-2$, è maggiore di k, dunque N supera $k\,(k-1$.

Osservazione. — Questo teorema contiene il seguente, dovuto a Serret:

Una funzione di k *lettere che ha più di* 2k *valori ne ha almeno* $\frac{k\,(k-1)}{2}$, se $k < 12$.

CAPO II.°

Limiti di transitività dei gruppi non alternati.

74. Teorema 1.° — *Se* $n+\nu$ *è il grado di un gruppo* G, *e se ciascuna delle sue sostituzioni non sposta meno di* $n+1$ *lettere,* G *non può essere* ν *volte transitivo, se non ha luogo la relazione*

$$1 \cdot 2 \cdot 3 \ldots (\nu-1) < n^\alpha,$$

indicando con α *il numero dei fattori primi uguali e disuguali di* $n+1$.

Dividiamo le $n+\nu$ lettere di G nei due sistemi $x_1, x_2, x_3, \ldots x_{\nu-1}$: $a_1, a_2, a_3, \ldots a_{n+1}$. G, essendo ν volte transitivo, deve contenere un gruppo transitivo H, formato dalle sostituzioni che spostano soltanto le lettere $a_1, a_2, a_3 \ldots a_{n+1}$. Ciascuna sostituzione di H deve spostare tutte le suddette lettere, pèrchè se fosse altrimenti G conterrebbe delle sostitozioni che sposterebbero meno di $n+1$ lettere, il che è contrario all'ipotesi, quindi H contiene la sola sostituzione 1 che non sposta una data lettera, dal che segue che H non possa contenere due sostituzioni S_p, S_q le quali ad una stessa lettera a_p facciano succedere la medesima lettera a_q, perchè se le contenesse, dovrebbe contenere l'altra $S_pS_q^{-1}$ la quale è diversa da 1 e non sposterebbe a_p, il che è impossibile. Inoltre, essendo H transitivo, può a_1 per le sostituzioni di H occupare un posto qualunque nella permutazione $a_1a_2 \ldots a_{n+1}$, quindi può occupare $n+1$ posti, ma l'ordine di un gruppo qualunque è uguale al prodotto del numero dei posti che può occupare una lettera pel numero delle sostituzioni che non spostano questa lettera, dunque l'ordine di H è $n+1$.

75. Le sostituzioni di G che spostano $x_1, x_2, \ldots x_{\nu-1}$ permutano queste lettere tra loro in tutt'i modi possibili, per essere G ν volte transitivo. Inoltre tali sostituzioni debbono essere della forma AB, A'B' etc., essendo A, A' etc. delle sostituzioni relative alle lettere $x_1, x_2 \ldots x_{\nu-1}$, e B, B' etc. delle sostituzioni relative alle rimanenti lettere; poichè, non potendo ν superare la metà di $n+\nu$ (33. Co. 2°), deve essere $\nu < n$, e quindi, per l'ipotesi fatta, G non può contenere sostituzioni che permutano soltanto le lettere $x_1, x_2, \ldots x_{\nu-1}$. Ora il gruppo $H' = (AB, A'B'_1 \ldots)$ deve soddisfare alle seguenti condizioni: 1° non deve contenere una sostituzione AB in cui B sia una sostituzione di H, poichè, se H contenesse B_1 conterrebbe anche B^{-1}, e quindi G dovrebbe contenere $ABB^{-1}=A$, il che è impossibile: 2° non deve contenere due sostitozioni AB, A'B' nelle quali B sia uguale a B', poichè, se così fosse, G conterrebbe la sostituzione $AB(A'B')^{-1}=AA'^{-1}$, il che è impossibile: 3° deve contenere il prodotto di una qualunque delle sue sostituzioni per una sostituzione qualunque di H: 4° se $A=A'$, il prodotto di AB per $(A'B')^{-1}$ deve appartenere ad H, perchè $AB(A'B')^{-1}$ appartiene a G e non sposta le lettere $x_1, x_2 \ldots x_{\nu-1}$. Da queste condizioni risulta che ad ogni sostituzione A corrispondono $n+1$ sostituzioni H, formate da una sostituzione B_1, non contenuta in H, e dai prodotti di B_1 per cia-

scuna delle sostituzioni di H, ma il numero delle sostituzioni A, A' etc. è $1 \cdot 2 \cdot 3 \ldots (\nu - 1)$, e quello delle sostituzioni di H è $n + 1$, dunque l'ordine del gruppo K, formato dalle sostituzioni B, è $(n + 1) \cdot 1 \cdot 2 \ldots (\nu - 1)$.

76. Le sostituzioni di K sono permutabili ad H; infatti, indicando con H_1 una sostituzione di H, si ha

$$BH_1B^{-1} = ABH_1(AB)^{-1},$$

ma questa sostituzione appartiene a G, per essere il prodotto di tre sostituzioni di questo gruppo, e non sposta le lettere $x_1, x_2 \ldots x_{\nu-1}$, dunque appartiene ad H. Di qui risulta che il gruppo L, che contiene tutte le sostituzioni possibili permutabili ad H, deve contenere K, e quindi l'ordine di L deve essere divisibile per $(n + 1) \cdot 1 \cdot 2 \cdot 3 \ldots (\nu - 1)$, che è l'ordine di K.

77. Ora ci proponiamo di trovare un limite in più dell'ordine di L. Quest'ordine è uguale al prodotto del numero dei sistemi di posti che per le sostituzioni di L possono occupare due lettere a_1, a_2 nella permutazione $a_1a_2a_3 \ldots a_{n+1}$, il quale è al più $n(n+1)$, pel numero delle sostituzioni di L che non spostano a_1 ed a_2 (29). Sia $S = (a_1a_2 \ldots)(a_{p+1} \ldots)$ la sostituzione di H che scambia a_1 con a_2, e sia p l'ordine del ciclo $(a_1a_2 \ldots)$, sarà p un divisore dell'ordine di S, e quindi un divisore dell'ordine $n + 1$ di H (17. Co. 2°). Una qualunque delle sostituzioni di L che non spostano a_1 ed a_2, che indichiamo con L', deve trasformare S in se stessa; poichè, se la trasformata fosse un altra sostituzione S' diversa da S, S' dovrebbe appartenere ad H, perchè tutte le sostituzioni di L sono permutabili ad H, e dovrebbe contenere un ciclo in cui le lettere a_1 ed a_2 fossero negli stessi posti che occupano in S, perchè la trasformata di S si ottiene, sostituendo a ciascuna lettera di S quella che le fa succedere L', ed L' fa succedere ad a_1 la stessa a_1 ed ad a_2 la stessa a_2; quindi, nell'ipotesi fatta, H conterrebbe due sostituzioni S ed S' che scambierebbero a_1 con a_2, il che è impossibile. Or poichè L' trasforma S in se stessa, e non sposta le lettere a_1 ed a_2 del ciclo $(a_1a_2 \ldots)$, non dovrà spostare le rimanenti $p - 2$ lettere di questo ciclo, quindi le sostituzioni di L che non spostano a_1 ed a_2 non possono far prendere ad una lettera a_{p+1}, non compresa nel detto ciclo, che $n + 1 - p$ posti diversi, laonde il numero delle sostituzioni di L che non spostano a_1 ed a_2 è al più uguale al prodotto di $n + 1 - p$ pel numero delle sostituzioni di L che non spostano a_1, a_2, a_{p+1}.

H deve contenere una sostituzione S' che fa succedere a_{p+1} ad a_1, ed il gruppo H' formato da S, da S' e dalle loro derivate, quindi se p' è l'ordine di H, sarà p' un divisore dell'ordine $n + 1$ di H, e siccome H' contiene S, sarà l'ordine di S un divisore di p', ma p è un divisore dell'ordine di S, dunque p è un divisore di p'. Le sostituzioni di L che non spostano a_1, a_2, a_{p+1}, trasformando S ed S' in se stesse, trasformeranno anche in se stesse le rimanenti sostituzioni di H', e quindi non sposteranno le p' lettere che le p' sostituzioni di H' fanno succedere ad a_1, laonde per queste sostituzioni di L una lettera a_q non può prendere che $n + 1 - p'$ posti, e perciò il loro numero è al più uguale al prodotto di $n + 1 - p'$ pel numero delle sostituzioni di L che non spostano a_1, a_2, a_{p+1}, a_q.

Seguitando allo stesso modo finchè si giunge alle sostituzioni che non spostano alcuna lettera, le quali si riducono alla sostituzione 1, si ha che l'ordine di L non può superare

$$n(n+1)(n+1-p)(n+1-p')\ldots 1;$$

ma questo numero deve essere divisibile per l'altro $(n+1)\cdot 1\cdot 2\cdot 3\ldots(\nu-1)$, dunque si ha

$$1\cdot 2\cdot 3\ldots(\nu-1) < n(n+1-p)(n+1-p')\ldots 1.$$

Ma i fattori del 2° membro di questa disuguaglianza sono, ad eccezione del 1°, minori di n, ed il loro numero non può superare il numero α dei fattori primi uguali e disuguali di $n+1$, perchè p, p' etc. sono divisori di $n+1$ e ciascuno è multiplo del precedente, dunque con più ragione si ha

$$1\cdot 2\cdot 3\ldots(\nu-1) < n^{\alpha}.$$

78. Teorema 2.° — *Se le sostituzioni di un gruppo G di* $n+\nu$ *lettere spostano meno di* $n+1$ *lettere, esso non può essere* ν *volte transitivo se non si verifica alcuna delle seguenti condizioni:*

1.° *per* $\nu \overset{=}{>} 4$, $\quad \dfrac{1\cdot 2\cdot 3\ldots\nu}{2} < n'^{\alpha}$,

essendo n' *un numero minore di* $n-1$, *ed* α *il numero dei fattori primi di* $n'+1$;

2.° *per* $\nu > 12$ $\quad \dfrac{\nu(\nu-1)}{2} \overset{=}{<} n$,

3.° *per* $\nu > 12$ $\quad \dfrac{2\nu-3}{q}\nu \overset{=}{<} n$,

essendo q *il numero primo immediatamente maggiore di* $\dfrac{n}{\nu}$,

4.° *per* $\nu < 12$ $\quad 2\nu \overset{=}{<} n$.

Dividiamo le $n+\nu$ lettere di G nei due sistemi $x_1, x_2, x_3\ldots x_\nu$; $a_1, a_2, a_3\ldots a_n$. G, essendo ν volte transitivo, contiene un gruppo intransitivo H, formato dalle sostituzioni che non spostano $x_1, x_2, x_3\ldots x_\nu$; e le lettere $a_1, a_2, a_3\ldots a_n$ si possono dividere in sistemi $a, a', \ldots$; $b, b', \ldots$; ... tali che le lettere di ciascuno siano tra loro permutate transitivamente dalle sostituzioni di H.

Le sostituzioni di G, che permutano $x_1, x_2\ldots x_\nu$, sono della forma AB, A'B' etc., essendo A, A' etc. delle sostituzioni che permutano in tutt'i modi possibili le dette lettere, e B, B' etc. delle sostituzioni che permutano $a_1, a_2\ldots a_n$. Indichiamo con I il gruppo formato dalle sostituzioni AB, A'B', etc. nelle quali A, A' etc. dinotano sostituzioni equivalenti ad un numero pari di trasposizioni fatte sulle lettere $x_1, x_2\ldots x_\nu$. Le sostituzioni di I sono permutabili ad H, infatti, se H' è una sostituzione di H, la trasformata di H' per mezzo di A'B' sarà

$$A'B'H'(A'B')^{-1} = A'A'^{-1}B'H'B'^{-1} = B'H'B'^{-1};$$

ma questa sostituzione appartiene a G e non sposta le lettere $x_1, x_2\ldots x_\nu$, quindi fa parte di H, e poichè le sostituzioni di H permutano tra loro le lettere di ciascun sistema, le sostituzioni di I debbono scambiare le lettere di un sistema con quelle di un altro.

79. Or supponiamo che il sistema $a, a', \ldots$ che intendiamo formato da $n'+\nu'$ lettere, soddisfi alle due seguenti condizioni: 1° che ogni sostituzione di I permuti le lettere di questo sistema con altre del medesimo sistema: 2° che ciascuna sostituzione di I, non contenuta in H, sposti delle lettere di questo sistema.

Le sostituzioni di H sono della forma $h'k'$, $h''k''$ etc., essendo h', h'' etc. delle sostituzioni sopra le lettere $a, a' \ldots$, e k', k'' etc. delle sostituzioni sopra le lettere dei rimanenti sistemi. Il gruppo transitivo $h = (h', h'', \text{etc.})$ non contiene il gruppo alternato corrispondente alle lettere $a, a', \ldots$ Infatti, se indichiamo con b lo spostamento fatto nelle lettere $a, a', \ldots$ dalla sostituzione AB di I, lo spostamento fatto nelle medesime lettere da A^2B^2 sarà b^2 ed equivarrà ad un numero pari di trasposizioni, or, se $b^2 = h'$, la sostituzione $A^2B^2 (h'k')^{-1}$ non sposterebbe le lettere del sistema $a, a', \ldots$, ma essa appartiene ad I, perchè fa parte di G e non sposta $x_1, x_2 \ldots$, quindi una sostituzione di I, non contenuta in H, non sposterebbe le lettere del sistema in parola, il che è contrario all'ipotesi fatta. dunque h, non potendo contenere la sostituzione b^2 corrispondente ad un numero pari di trasposizioni fatte sopra $a, a', \ldots$, non contiene il gruppo alternato di queste lettere.

80. Supponiamo che h sia n' volte transitivo, e che le sue sostituzioni non spostino meno di $n'+1$ lettere. Dividiamo le lettere $a, a', \ldots$ nelle due classi $y_1, y_2, y_3 \ldots y_{\nu'-1}$; $a_1, a_2, a_3 \ldots a_{n'+1}$. Le sostituzioni di h che non spostano le lettere della 1ª classe formano un gruppo g semplicemente transitivo, perchè h è ν' volte transitivo e le sostituzioni di g lasciano fisse $\nu' - 1$ lettere. L'ordine di g è $n' + 1$, ed il numero delle sostituzioni fatte sulle lettere della 2ª classe e permutabili a g non può superare $(n'+1)\, n'^{\alpha'}$, dinotando con α' il numero dei fattori primi di $n'+1$.

Indichiamo con g_1, g_2 etc. le sostituzioni di g, e con G_1, G_2 etc. le $n'+1$ sostituzioni corrispondenti di H. Sia A'B' una sostituzione di I che scambia $y_1, y_2 \ldots y_{\nu'-1}$ rispettivamente coll'altre $z_1, z_2 \ldots z_{\nu'-1}$. Il gruppo h, essendo ν' volte transitivo, contiene una sostituzione h' che scambia $z_1, z_2 \ldots z_{\nu'-1}$, rispettivamente con $y_1, y_2 \ldots y_{\nu'-1}$, perciò, dinotando con H' la sostituzione di H che produce lo spostamento h', l'altra A'B'H' non sposta le lettere $y'_1, y'_2 \ldots y'_{\nu'-1}$, e lo stesso succede per le $n'+1$ sostituzioni A'B'H'G$_1$, A'B'H'G$_2$ etc., le quali producono nelle lettere $a_1, a_2, \ldots a_{n'+1}$ gli spostamenti βg_1, βg_2 etc., indicando con β lo spostamento fatto in queste lettere da A'B'H'. Similmente se indichiamo con A''B'' un'altra sostituzione di I, in cui A'' è diversa da A', e dinotiamo con H'' una sostituzione di H che produce per le lettere $y_1, y_2, \ldots y_{\nu'-1}$ uno spostamento contrario a quello formato da A''B'' per le medesime lettere, A''B''H'' non sposterà $y'_1, y'_2 \ldots y'_{\nu'-1}$, come anche l'altre $n'+1$ A''B''H''G$_1$, A''B''H''G$_2$ etc., le quali producono nelle lettere $a_1, a_2 \ldots a_{n'+1}$ gli spostamenti $\beta' g_1$, $\beta' g_2$ etc., indicando con β' lo spostamento operato nelle medesime lettere da A''B''H''. Seguitando allo stesso modo, si avranno tante serie di $n'+1$ sostituzioni analoghe alle già formate

$$\beta g_1, \beta g_2, \ldots ; \beta' g_1, b' g_2, \ldots$$

quante sono le sostituzioni diverse A', A', etc., ossia $\frac{1.2.3 \ldots \nu}{2}$ serie.

Tutte le sostituzioni βg_1 etc. di una medesima serie sono evidentemente diverse, e lo sono anche due sostituzioni appartenenti a serie diverse; infatti se si avesse $\beta g_1 = \beta' g_2$, la sostituzione

$$A'B'H'G_1 (A''B''H''G_2)^{-1} = A'A''^{-1} (B'H'G_1)(B''H''G_2)^{-1},$$

la quale appartiene ad I e non ad H, spostando le lettere $x_1, x_2, \dots x_{\nu'-1}$, lascierebbe immobili le lettere $a_1, a_2, \dots a_{n'+1}$, il che è contrario all'ipotesi fatta.

Le sostituzioni $\beta g_1 \dots, \beta' g_1 \dots, \dots$ sono permutabili al gruppo g. Infatti se indichiamo con H_p una sostituzione del gruppo K, formato dalle sostituzioni di H che non spostano $y_1, y_2, \dots y_{\nu'-1}$, la trasformata di H_p per mezzo di $A'B'H'G$, sarà una sostituzione di G che non sposterà $x_1, x_2 \dots x_\nu$, e neppure l'altre $y_1, y_2, \dots y_{\nu'-1}$, perciò sarà una sostituzione di K, ma possiamo porre $A'B'H'G_1 = \alpha\beta g_1$, ed $H_p = \alpha' g_2$, indicando con α ed α' gli spostamenti prodotti da $A'B'H'G_1$ e da H_p nelle lettere diverse da $a_1, a_2, \dots a_{n'+1}$, perciò l'indicata trasformata può essere rappresentata nel modo seguente

$$\alpha\beta g_1 \, \alpha' g_2 (\alpha\beta g_1)^{-1} = \alpha\alpha'\alpha^{-1}\beta g_1 (g_n)(\beta g_1)^{-1},$$

donde si rileva che $\beta g_1 (g_2)(\beta g_1)^{-1}$ debba essere una sostituzione fatta sopra $a_1, a_2 \dots a_{n'+1}$, ossia che debba essere una sostituzione di g, dunque le $(n'+1)\frac{1.2.3\dots\nu}{2}$ sostituzioni βg_1, βg_2 etc. sono permutabili a g, e perciò deve essere

$$(n'+1)\frac{1.2.3\dots\nu}{2} \overset{=}{<} (n'+1)\, n'^{x'},$$

donde

$$\frac{1.2.3\dots\nu}{2} \overset{=}{<} n'^{x'},$$

essendo $n' < n' + \nu'$ od $n' + \nu' < n$ donde $n' < n - 1$.

81. Or supponiamo che le sostituzioni di h spostino meno di $n' + 1$ lettere. Dividiamo le lettere di h nelle due classi $y_1, y_2, \dots y_{\nu'}$; $a_1, a_2 \dots a_{n'}$. Le sostituzioni di h che non spostano le lettere della 1ª classe formano un gruppo intransitivo, perchè h è ν' volte transitivo, per conseguenza è pure intransitivo per rispetto ad $a_1, a_2 \dots a_{n'}$ il gruppo H_1 formato dalle sostituzioni di H che non spostano $y_1, y_2, \dots y_\nu$, ma se un gruppo è intransitivo per rispetto ad alcune delle sue lettere, lo è anche per rispetto al complesso di tutte le sue lettere, dunque H_1 è intransitivo per rispetto alle $n + \nu$ lettere di G, escludendovi $x_1, x_2 \dots x_\nu$; $y_1, y_2 \dots y_{\nu'}$ che restano immobili nelle sostituzioni di H_1.

Lo sostituzioni del gruppo I_1, formato dalle sostituzioni di I che non spostano $y_1, y_2 \dots y_{\nu'}$, sono permutabili ad H_1. Infatti sia $A'B'$ una sostituzione di I_1 ed H' una sostituzione di H_1, la trasformata di H' per mezzo di $A'B'$ è

$$A'B'H' (A'B')^{-1} = A'A'^{-1}B'H'B'^{-1} = B'H'B'^{-1},$$

ma essa appartiene a G, non sposta $x_1, x_2 \dots x_\nu$ e nemmeno $y_1, y_2 \dots y_{\nu'}$, perchè B' ed H' non contengono queste lettere, dunque essa appartiene ad H_1.

Inoltre le sostituzioni di I_1 permutano in tutt'i modi possibili le lettere $x_1, x_2 \ldots x_\nu$. Invero indichiamo con A' uno spostamento di queste lettere, e con $A'B'$ la sostituzione corrispondente di I. Supponiamo che $A'B'$ scambii $y_1, y_2 \ldots y_\nu$ con $z_1, z_2 \ldots z_{\nu'}$ H, essendo ν' volte transitivo per rispetto ad $a_1, a_2 \ldots a_{n'}$, contiene una sostituzione H' che scambia $z_1, z_2 \ldots z_{\nu'}$ con $y_1, y_2 \ldots y_\nu$, quindi la sostituzione $A'B'H'$ non sposta $y_1; y_2, \ldots y_{\nu'}$, ma essa appartiene ad I, dunque fa parte di I_1, ma essa permuta le lettere $x_1, x_2 \ldots x_\nu$ secondo la sostituzione A', dunque le sostituzioni di I_1 permutano in tutt'i modi possibili le lettere $x_1, x_2 \ldots x_\nu$.

Or se dalle $n+\nu$ lettere di G escludiamo $x_1, x_2 \ldots x_\nu$; $y_1, y_2 \ldots y_\nu$, le rimanenti possono essere divise in sistemi tali che le lettere di ciascuno siano tra loro permutate dalle sostituzioni di H_1, per essere questo gruppo intransitivo per rispetto all'anzidette lettere. E siccome H_1 è permutabile a tutte le sostituzioni di I_1, queste scambiano le lettere di ciascun sistema con quelle di un altro.

Se tra questi sistemi ve n'è uno che soddisfa alle due condizioni: 1° che per ciascuna sostituzione di I_1 le lettere di questo sistema sono scambiate con altre dello stesso sistema: 2° che ogni sostituzione di I_1 non compresa in H_1 sposta delle lettere di questo sistema: allora ragionando sopra H_1 ed I_1 come si è fatto sopra H ed I, si perviene ad un limite simile a quello innanzi stabilito, ovvero si hanno altri due gruppi H_2 ed I_2, condizionati come H_1 ed I_1, le cui sostituzioni oltre le lettere $y_1, y_2 \ldots y_{\nu'}$ non spostano l'altre $z_1, z_2 \ldots z_{\nu'}$. Si può ragionare sopra H_2 ed I_2 come si è fatto su di H ed I, e così di seguito. Continuando questo ragionamento necessariamente si deve giungere o ad un limite simile a quello già dato, ovvero a due gruppi H_n ed I_n tali che dividendo le lettere del gruppo intransitivo H_n in sistemi, non vi sia alcuno di questi sistemi che soddisfi alle due condizioni innanzi riferite, poichè altrimenti vi sarebbe una serie indefinita di gruppi H_1, H_2 etc. nei quali il numero delle lettere va sempre diminuendo, e quindi vi sarebbe un numero indefinito di numeri minori di n, il che è impossibile.

Supponiamo che s'incontrino i due gruppi H_n ed I_n innanzi detti. Allora i sistemi in cui si dividono le lettere di H_n si possono distinguere in due categorie, raccogliendo nella 1ª quei sistemi tali che le lettere di ciascuno sono scambiate con lettere del medesimo sistema dalle sostituzioni di I_n, e nella 2ª quei sistemi le cui lettere sono scambiate con quelle di un altro da alcune sostituzioni di I_n.

82. I_n *contiene delle sostituzioni che non spostano le lettere di tutt'i sistemi della* 1ª *categoria*.

Siano S, S_1, S_2 etc. questi sistemi. Per ciascuno di essi vi debbono essere delle sostituzioni di I_n che non spostano le sue lettere, altrimenti vi sarebbe un sistema le cui lettere sarebbero permutate da tutte le sostituzioni di I_n, il che è contrario all'ipotesi fatta. Or sia A_1B_1 una sostituzione di I_n che non sposta le lettere di S. Le trasformate di A_1B_1 per mezzo delle altre sostituzioni di I_ν nemmeno spostano queste lettere, perchè le sostituzioni di I_n fanno succedere alle lettere di S altre lettere dello stesso S, e siccome A_1B_1 non contiene le lettere di S, le trasformate di A_1B_1, che si ottengono sostituendo alle lettere contenute in A_1B_1 quelle che a queste fanno succedere le sostituzioni trasformanti, neppure contengono le lettere

di S, e lo stesso succede di tutte le derivate A_1B_1, $A'_1B'_1$ etc. di queste trasformate. Queste derivate formano un gruppo il quale è contenuto in I_n ed è permutabile alle sue sostituzioni, quindi anche il gruppo $(A_1, A'_1 ...)$, formato dagli spostamenti che A_1B_1, $A'_1B'_1$ etc. producono nelle lettere x_1, x_2 etc. è contenuto nell'altro $(A, A', ...)$, formato dagli spostamenti che le sostituzioni di I_n fanno nelle medesime lettere, ed è permutabile alle sue sostituzioni, ma il gruppo (A, A' etc.) non può contenere un'altro gruppo a cui le sue sostituzioni siano permutabili (33), dunque deve essere (A, A' etc.) identico ad $(A_1, A'_1$ etc.).

Sia A'B' una sostituzione di I_n che non sposta le lettere di S_1, ed A_1 una sostituzione di $(A_1, A'_1$ etc.) non mutabile con A'. La sostituzione

$$(A'B')^{-1}(A_1B_1)^{-1}A'B'A_1B_1 = A_2B_2$$

non sposta le lettere dei due sistemi S ed S_1, poichè se A'B' spostasse le lettere di S, non contenendosi queste lettere in $(A_1B_1)^{-1}$, la permutazione fatta sulle lettere di S da A'B' verrebbe distrutta dalla permutazione contraria fatta da $(A'B')^{-1}$, quindi A_2B_2 non sposta le lettere di S, similmente si dimostrerebbe che non sposta quelle di S_1. E poichè A_2B_2 produce nelle lettere x_1, x_2 etc. lo spostamento indicato da $A'^{-1}A_1^{-1}A'A_1$, che è diverso da 1, per essere A' ed A_1 due sostituzioni non permutabili tra loro, A_2B_2 appartiene ad I_n e non ad II_n. Le trasformate di A_2B_2 per mezzo delle sostituzioni di I_n, e le loro derivate A_2B_2, $A'_2B'_2$ etc. non spostano le lettere di S e di S_1, ed il gruppo $(A_2, A'_2$ etc.) è identico ad (A, A' etc.).

Nello stesso modo si potrebbero formare delle sostituzioni A_3B_3, $A'_3B'_3$ etc. le quali non spostassero le lettere di S, S_1, S_2, ed il gruppo $(A_3, A'_3$ etc.) sarebbe identico ad (A, A', etc.), e continuando nella stessa guisa si giungerebbe a trovare delle sostituzioni di I_n che non sposterebbero le lettere di tutt'i sistemi della 1ª categoria.

La proposizione dimostrata conduce alle due seguenti.

83. *Le sostituzioni di I_n si ricavano dalle sostituzioni di I_n che non spostano le lettere dei sistemi di 1ª categoria e dalle sostituzioni di II_n.*

Supponiamo che i sistemi di 1ª categoria siano i tre S, S_1, S_2, e quindi A_3B_3, $A'_3B'_3$ etc. le sostituzioni di I_n che non spostano le lettere dei sistemi di 1ª categoria, inoltre sia A' la sostituzione di (A, A'...) che è identica alla sostituzione A_3 del gruppo $(A_3, A'_3 ...)$. La sostituzione

$$A'B'(A_3B_3)^{-1} = B'B_3^{-1}$$

appartiene ad I_n, ed anche ad II_n, perchè non sposta le lettere x_1, x_2 etc. Or, ponendo $B'B_3^{-1} = C$, si ha $A'B'(A_3B_3)^{-1} = C$, donde $A'B' = C \cdot A_3B_3$, il che dimostra la proposizione

84. *Vi esistono sistemi di 2ª categoria.*

Se questi non esistessero, le sostituzioni A_3B_3, $A'_3B'_3$ etc. sposterebbero le sole v lettere $x_1, x_2 ...$, il che è impossibile, perchè le sostituzioni di un gruppo v volte transitivo debbono spostare più di v lettere (30).

85. Dividiamo i sistemi di 2ª categoria in classi, raccogliendo nella medesima classe quelli che sono transitivamente permutati dalle sostituzioni di I_n, e che perciò

sono formati dallo stesso numero di lettere, allora possiamo stabilire la seguente proposizione

Ogni sostituzione di I_n non contenuta in H_n sposta dei sistemi di ciascuna classe.

Indichiamo con Γ una di queste classi, e supponiamo che la sostituzione $A'B'$ di I_n, non contenuta in H_n, non sposti i sistemi di Γ. Poichè le sostituzioni di I_n scambiano i sistemi di Γ con altri sistemi della stessa Γ, ed $A'B'$ non contiene scambii di questi sistemi, neppure ve ne saranno nelle trasformate di $A'B'$ per mezzo delle sostituzioni di I_n e nelle derivate da queste trasformate, $A_2B_2, A'_2B'_2$ etc. Ora con un ragionamento analogo a quello fatto antecedentemente si dimostrerebbe che $(A_2, A'_2$ etc.) sarebbe identico ad $(A, A'$, etc.), e che I_n risulterebbe dalle sostituzioni $A_2B_2, A'_2B'_2$ etc. e da quelle di H_n, ma questo è impossibile, perchè nè le sostituzioni $A_2B_2, A'_2B'_2$ etc. nè quelle di H_n permutano i sistemi di Γ, mentre questi sistemi sono permutati transitivamente dalle sostituzioni di I_n, dunque è falsa l'ipotesi che vi siano in I_n delle sostituzioni che non spostano i sistemi di una classe.

Se indichiamo con E, E' etc. gli spostamenti dei sistemi di Γ prodotti dalle sostituzioni $AB, A'B'$ etc. di I_n, sarà $E = E'$, se $A = A'$, e viceversa. Infatti lo spostamento prodotto negli anzidetti sistemi da $AB(A'B')^{-1}$ è EE'^{-1}, ma $AB(A'B')^{-1}=BB'^{-1}$, appartenendo ad H_n, non può dare spostamenti di sistemi, quindi $EE'^{-1}=1$, donde $E=E'$. Se $E=E'$, dovrà essere $EE'^{-1}=1$, e quindi $AB(A'B')^{-1}$ dovrà appartenere ad H_n, il che importa che si abbia $AA'^{-1}=1$ donde $A=A'$.

Da questa proposizione risultano le due seguenti:

86. *Indicando con μ il numero dei sistemi di Γ, deve essere*

$$\frac{1\cdot2\cdot3\ldots\nu}{2} \overset{=}{<} 1\cdot2\ldots\mu$$

donde

$$\nu \overset{=}{<} \mu.$$

Poichè il numero delle sostituzioni A, A' etc. è $\frac{1\cdot2\cdot3\ldots\nu}{2}$, e quello delle permutazioni dei μ sistemi di Γ non può superare $1\cdot2\ldots\mu$.

87. *Il gruppo $(E, E'\ldots)$ è transitivo ed isomorfo senza meriedria all'altro $(A, A'\ldots)$.*

Infatti ad ogni sostituzione A corrisponde una sostituzione E, od al prodotto di due sostituzioni A corrisponde il prodotto delle sostituzioni corrispondenti E.

88. Or poichè il gruppo $(E, E'\ldots)$ è isomorfo all'altro $(A, A'\ldots)$, vi deve essere una funzione F_1, di $x_1, x_2 \ldots x_\nu$ tale che, se s'indicano con $F_1, F_2, F_3\ldots$ i valori diversi che assume quando sulle sue lettere si operano le sostituzioni di $(A, A'$ etc.), e nelle sostituzioni E, E' etc. si scambiano convenientemente i sistemi di Γ colle lettere F_1, F_2 etc., si hanno le sostituzioni per mezzo delle quali dalla permutazione $F_1F_2F_3\ldots$ si passa a quelle che si ottengono operando sulle lettere $x_1 x_2$ etc. di ciascuno dei fattori F_1, F_2 etc. le sostituzioni di $(A, A'$ etc.). Quindi il numero μ

dei sistemi di Γ deve essere uguale al numero dei valori diversi di F_1, e perciò uguale al quoziente di $\frac{1\cdot 2\cdot 3 \ldots \nu}{2}$, ordine del gruppo (A, A' etc.), pel numero delle sostituzioni di (A, A', etc.) che non alterano F_1. Possono darsi due casi: 1° che tra le funzioni corrispondenti alle diverse classi ve n'esista almeno una che non sia simmetrica per rispetto a $\nu - 1$ delle lettere $x_1, x_2 \ldots x_\nu$: 2° che tutte le funzioni corrispondenti alle diverse classi siano simmetriche per rispetto a $\nu - 1$ delle dette lettere.

89. 1° Caso. — Sia la funzione F_1, corrispondente alla classe Γ, non simmetrica per rispetto a $\nu - 1$ lettere. Se F_1 è simmetrica o alternata per rispetto a $\nu - 2$ lettere e non simmetrica per rispetto alle due rimanenti, essa non deve variare per tutte le sostituzioni del gruppo alternato fatte sulle $\nu - 2$ lettere per rispetto a cui è simmetrica o alternata, ed il loro numero è $\frac{1\cdot 2\cdot 3 \ldots (\nu - 2)}{2}$. Ma se F_1, essendo simmetrica per rispetto a $\nu - 2$ lettere, è simmetrica per rispetto alle due rimanenti lettere, essa non varia per le $\frac{1\cdot 2 \ldots (\nu - 2)}{2}$ anzidette sostituzioni, come anche per quelle che si ottengono moltiplicando per la trasposizione formata dalle due lettere rimanenti per ciascuna delle sostituzioni formate da un numero impari di trasposizioni fatte sulle $\nu - 2$ lettere, ma queste sono $\frac{1\cdot 2 \ldots \nu - 2}{2}$, quindi in questo caso F_1 non varia per $1\cdot 2 \ldots (\nu - 2)$ sostituzioni del gruppo alternato (A, A'...). Se F_1 non è simmetrica nè alternata per rispetto a $\nu - 2$ lettere, ed è $\nu > 12$, il numero dei valori che può prendere è superiore a $\nu(\nu - 1)$ (73), perciò il numero totale delle sostituzioni che non alterano F_1 è minore di $1\cdot 2 \ldots (\nu - 2)$, e con più ragione è minore di questo numero quello delle sostituzioni del gruppo alternato che non alterano F_1. Quindi se $\nu > 12$, sarà

$$\mu \overset{=}{>} \frac{\nu(\nu - 1)}{2},$$

ma $\mu \overset{=}{>} \nu$ (85) e $\nu \overset{=}{<} n$, dunque sarà

$$n \overset{=}{>} \frac{\nu(\nu - 1)}{2},$$

90. 2° Caso. — Essendo F_1 simmetrica o alternata per rispetto a $\nu - 1$ lettere, il numero delle sostituzioni del gruppo alternato (A, A', etc.) che non l'alterano è $\frac{1\cdot 2\cdot 3 \ldots (\nu - 1)}{2}$, quindi deve essere $\mu = \nu$. Similmente, se indichiamo con μ', μ'' etc. i numeri dei sistemi che compongono l'altre classi, deve essere $\mu' = \mu'' = \ldots = \nu$.

91. Or, se indichiamo con m, m', m'' etc. i numeri delle lettere che compongono i sistemi delle diverse classi, e supponiamo che m sia il più grande di essi, possiamo distinguere due casi: 1° che non esista alcun numero primo minore di ν e maggiore di m: 2° che esistano dei numeri primi che soddisfano alla detta condizione.

92. 1° Caso. — Tra ν e $\frac{\nu-1}{2}$ esiste sempre un numero primo (Serret Algebra superiore Se. III. Ca. IV.), perciò sarà $m > \frac{\nu-1}{2}$, e con più ragione

$$(m + m' + m'' + \ldots)\,\nu > \frac{\nu(\nu-1)}{2},$$

ma $$(m + m' + m'' + \ldots)\,\nu = m\mu + m'\mu' + \ldots \overset{=}{<} n,$$

dunque sarà $$n \overset{=}{>} \frac{\nu(\nu-1)}{2},$$

93. 2° Caso. — Indichiamo con p il più piccolo numero primo minore di ν e maggiore di m. Poichè il gruppo alternato (A, A', etc.) contiene tutte le sostituzioni equivalenti ad un numero pari di trasposizioni, conterrà la sostituzione circolare formata da p qualunque delle lettere $x_1, x_2 \ldots x_\nu$. Sia A'B' questa sostituzione. A'B' permuta circolarmente p sistemi di Γ, e di ciascun' altra classe. Infatti se F_1 non è simmetrica per rispetto ad x_1, F_2 lo sarà per rispetto ad un' altra lettera x_2, F_3 lo sarà per rispetto ad una terza lettera x_3, e così di seguito, ma lo scambio di due valori di F_1 corrisponde allo scambio di due sistemi di Γ, quindi A'B' permuta circolarmente p sistemi di Γ. Similmente si dimostrerebbe che A'B' permuta circolarmente p sistemi di ciascun altra classe. Ma A'B' oltre dello spostare circolarmente p sistemi di ciascuna classe, potrebbe permutare tra loro le lettere di alcuni sistemi. Indichiamo con ω, ω', ω'' etc. gli ordini dei cicli che producono queste permutazioni. Poichè ω, ω' etc. al più sono uguali ad m, saranno primi con p, quindi il loro minimo multiplo, che indichiamo con ρ, sarà primo con p, donde segue che la sostituzione $(A'B')^\rho$ sposterà p delle lettere x_1, x_2 etc., e, permutando circolarmente p sistemi di ciascuna classe, sposterà $pm + p'm' +$ etc. delle lettere $a_1, a_2 \ldots$, perciò in tutto sposterà $p + pm + p'm' +$ etc. lettere. Ma ogni sostituzione del gruppo (AB, A'B') non può spostare meno di $2\nu - 3$ lettere (31), dunque sarà

$$p\,(1 + m + m' + \ldots) \overset{=}{>} 2\nu - 3,$$

donde $$m + m' + \ldots \overset{=}{>} \frac{2\nu - 3}{p} - 1,$$

e quindi $$(m + m' + \ldots)\,\nu \overset{=}{>} \left(\frac{2\nu - 3}{p} - 1\right)\nu.$$

ma $$(m + m' + \ldots)\,\nu = m\mu + m'\mu' + \ldots \overset{=}{<} n\,;$$

dunque sarà $$n \overset{=}{<} \left(\frac{2\nu - 3}{p} - 1\right)\nu.$$

Ma essendo q il numero primo immediatamente superiore a $\frac{n}{\nu}$, esso sarà maggiore di $m + m' + \ldots$, e perciò almeno uguale a p, adunque con più ragione si avrà

$$n \overset{=}{>} \left(\frac{2\nu - 3}{q} - 1\right)\nu.$$

94. Se $\nu < 12$ ed uno dei numeri m, m' etc. è maggiore di 1, sarà

$$m\mu + m'\mu' + \ldots \overset{=}{>} (m + m' + \ldots)\nu \overset{=}{>} 2\nu.$$

Ma se tutt'i numeri m, m' etc. sono uguali ad 1, le sostituzioni di Π_n non sposteranno le lettere delle diverse classi, ma debbono spostare almeno $2\nu-3$ lettere (31), dunque le lettere che compongono queste classi debbono essere al più $n-2\nu+3$, quindi sarà

$$m\mu + m'\mu' + \ldots \overset{=}{<} n - 2\nu + 3,$$

ovvero, essendo $\mu = \mu' = \ldots = \nu$,

$$(m + m' + \ldots)\nu \overset{=}{<} n - 2\nu + 3,$$

donde si ha la relazione

$$n \overset{=}{>} \nu\,(m + m' + \ldots + 2)\,\nu - 3 \overset{=}{>} 2\nu$$

la quale si verifica anche nel caso che i numeri m, m' etc. si riducono ad un solo, essendo $\nu > 4$.

Se $\nu > 7$ ed $m \overset{=}{>} 3$, essendo

$$m\mu + m'\mu' + \ldots = (m + m' \ldots)\,\nu \overset{=}{<} n,$$

sarà $$n \overset{=}{>} 3\nu.$$

Ma se $m < 3$ o $\nu > 7$, essendo il numero primo immediatamente superiore ad $\frac{n}{6}$ almeno uguale a 3, sarà almeno

$$\frac{2\nu - 3}{q} > \frac{12}{3} = 4,$$

e quindi sarà anche $$n > 3\nu.$$

PARTE SECONDA

PROPRIETÀ DELLE CONGRUENZE RELATIVE ALLE SOSTITUZIONI LINEARI

CAPO 1.°

Teorica di Galois.

95. Una funzione intera $F(x)$ dicesi *divisibile per un altra* $f(x)$ *secondo il modulo primo* p se si ha la relazione

$$F(x) = f(x)\,\varphi(x) + p\psi(x),$$

essendo $\varphi(x)$ e $\psi(x)$ due funzioni intere.

Una funzione intera $F(x)$ dicesi *irriducibile secondo il modulo* p quando non è divisibile per alcuna funzione intera di grado inferiore al suo ed il coefficiente della più alta potenza di x è uguale ad 1.

Dividendo una funzione intera $F(x)$ per un'altra irriducibile $f(x)$ di grado ν si ha un resto che può essere rappresentato da $\varphi(x) + p\psi(x)$, essendo $\varphi(x)$ un polinomio nel quale il grado è al più $\nu - 1$, ed i coefficienti dei numeri compresi tra 0 e p. Chiameremo $\varphi(x)$ *il valore ridotto di* $F(x)$ *secondo il modulo* p *e secondo la funzione modulare* $f(x)$.

La funzione $\varphi(x)$, essendo della forma

$$a_0 x^{\nu-1} + a_1 x^{\nu-2} + \ldots\ldots$$

e potendo i coefficienti a_0, a_1 etc. variare da 0 a p, può assumere p^ν valori diversi tra i quali si comprendono i seguenti

$$0,\ 1,\ 2,\ \ldots\ldots\ p-1,$$

quindi se si esclude 0, si hanno $p^\nu - 1$ funzioni ridotte secondo il modulo p e secondo la funzione modulare $f(x)$.

96. Teorema 1.° — *Se il prodotto delle due funzioni intere* $F(x)$, $F_1(x)$ *è divisibile secondo il modulo* p *per la funzione irriducibile* $f(x)$, *una di esse deve esser divisibile per* $f(x)$.

È evidente che se $F(x)$ ed $F_1(x)$ ammettono un divisore comune, questo debba dividere il resto della loro divisione, e viceversa, quindi si cercherà il massimo co-

(*) Abbiamo creduto opportuno di esporre immediatamente prima del trattato delle sostituzioni lineari tutte quelle cognizioni sulle congruenze a modulo primo che servono ad esso di sostrato. Gli Autori che ci hanno servito per la compilazione di questa 2ª parte sono Serret *Cours d'Algebre superieure*, Derichlet *Vorlesungen über Zahlen theorie*. Jordan *Traité des substitutions*.

mun divisore di $F(x)$ ed $F_1(x)$ per mezzo della divisione. Di qui risulta che, essendo $f(x)$ una funzione irriducibile, il massimo comun divisore tra $F(x)$ ed $f(x)$ non possa essere che uno, supposto che la prima non sia divisibile per la seconda, e perciò il massimo comun divisore tra $F(x)\,F_1(x)$ ed $F_1(x)\,f(x)$ non sarà che $F_1(x)$; ma i due prodotti $F(x)\,F_1(x)$ ed $F_1(x)\,f(x)$ sono ambedue divisibili per $f(x)$, dunque lo dovrà essere anche il loro massimo comun divisore, donde si deduce che $F_1(x)$ dovrà esser divisibile per $f(x)$.

Corollario. — *Una funzione $F(x)$ non irriducibile può in un sol modo esser scomposta in fattori irriducibili.*

Infatti supponiamo che si abbia

$$aF(x) \equiv f(x)\,f_1(x)\,f_2(x)\ldots \equiv \varphi(x)\,\varphi_1(x)\,\varphi_2(x)\ldots \pmod p.$$

essendo a un numero che moltiplicato pel coefficiente della più alta potenza di x in $F(x)$ dia un prodotto congruo ad 1.

Ogni fattore del 1° prodotto divide il 2°, quindi dovrà dividere uno dei suoi fattori, ma questi sono tutti irriducibili, dunque deve essere uguale ad uno di essi. Analogamente si dimostrerebbe che ogni fattore del 2° dovrà avere il suo uguale nel 1°, dunque i due prodotti saranno identici.

97. Teorema 2.° — *Siano $X_1, X_2 \ldots X_m$ delle funzioni di x ridotte secondo il modulo p e la funzione modulare $f(x)$, ed $F(X)$ una funzione intera di X di grado m, avendo per coefficienti delle funzioni intere di x. Se $F(X_1), F(X_2) \ldots\ldots F(X_m)$ sono tutti divisibili per $f(x)$, si avrà identicamente*

$$F(X) = A_0(X - X_1)(X - X_2)\ldots(X - X_m) + f(x)\,\varphi(X, x) + p\,\varphi_1(X, x),$$

essendo $\varphi(X, x)$ e $\varphi_1(X, x)$ due funzioni di X, ed x a coefficienti interi, ed A_0 il coefficiente del 1° termine di $F(X)$.

Dividiamo $F(X)$ per $X - X_1$ ed indichiamo con $F_1(X)$ il quoziente e con R_1 il residuo; indi dividiamo $F_1(X)$ per $X - X_2$, ed indichiamo con $F_2(X)$ il quoziente e con R_2 il residuo, e così di seguito. Si avranno l'uguaglianze

$$F(X) = (X - X_1)\,F_1(X) + R_1$$
$$F_1(X) = (X - X_2)\,F_2(X) + R_2$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$F_{m-1}(X) = (X - X_m)\,A_0 + R_m.$$

Sostituendo il valore di $F_{m-1}(X)$ in quello di $F_{m-2}(X)$, indi il valore risultante di $F_{m-2}(X)$ in $F_{m-3}(X)$, e così di seguito, si avrà un uguaglianza della forma

$$F(X) = A_0(X - X_1)(X - X_2)\ldots(X - X_m) + \Theta(X, x),$$

essendo $\Theta(X, x) = R_1 + R_2(X - X_1) + \ldots + R_m(X - X_1)\ldots(X - X_{m-1})$,

ma $R_1, R_2, \ldots R_m$ sono divisibili per $f(x)$, essendo divisibili per $f(x)$ i risultati che si ottengono sostituendo $X_1, X_2 \ldots X_m$ in luogo di X in $F(X)$, dunque dovrà essere $\Theta(X, x)$ divisibile per $f(x)$, ossia sarà

$$\Theta(X, x) = f(x)\,\varphi(X, x) + p\varphi_1(X, x),$$

onde si deduce l'uguaglianza proposta.

Corollario. — *Non vi può essere un'altra funzione ridotta* X' *diversa da* $X_1, X_2 \dots X_m$ *chè sostituita in luogo di* X *in* F(X) *dia un risultato divisibile per* $f(x)$
Infatti se vi fosse, dovrebbe essere

$$F(X') = A_0(X' - X_1)(X' - X_2) \dots (X' - X_m) + f(x)\varphi(X', x) + p\varphi_1(X', x),$$

ma F(X') è divisibile per $f(x)$, dunque lo dovrebbe essere anche il 2° membro, il che non è, perchè nessuno dei fattori del prodotto

$$(X' - X_1)(X' - X_2) \dots\dots (X' - X_m)$$

è divisibile per $f(x)$.

98. Se $F(x)$ dinota una funzione intera di x a coefficienti interi, diremo radice reale della congruenza

$$F(x) \equiv 0 \pmod p$$

ogni numero che sostituito in luogo di x rende $F(x)$ divisibile per p.

Se $f(x)$ dinota una funzione irriducibile, la congruenza

$$f(x) \equiv 0 \pmod p$$

non può avere alcuna radice reale; poichè se ne avesse una, indicandola con a; sarebbe $f(a) \equiv 0 \pmod p$, ma $f(x) - f(a)$ è divisibile per $x - a$, quindi se s'indica con M il quoziente sarebbe

$$f(x) - f(a) = M(x - a)$$

ovvero

$$f(x) \equiv M(x - a) \pmod p$$

il che è impossibile.

Ora, secondo l'idea di Galois, introduciamo nel calcolo un simbolo immaginario i tale che sia

$$f(i) \equiv 0 \pmod p,$$

e chiamiamo numeri complessi i risultati che si ottengono sostituendo i in luogo di x nelle funzioni ridotte secondo il modulo p e la funzione modulare $f(x)$, e radice immaginaria di

$$f(x) \equiv 0 \pmod p$$

ogni numero complesso che posto in luogo di x in $f(x)$ da un risultato divisibile per $f(i)$.

Ciò posto, se scomponendo $F(x)$ in fattori irriducibili si ha

$$aF(x) \equiv f_1(x)\, f_2(x)\, f_3(x) \dots\dots$$

la congruenza

$$F(x) \equiv 0 \pmod p$$

si scinderà nell'altra $f_1(x) \equiv 0,\quad f_2(x) \equiv 0,\quad f_3(x) \equiv 0 \dots\dots \pmod p$,

ma ciascuna di questa congruenza non può ammettere un numero di radici maggiore del suo grado (97), quindi la proposta congruenza non può avere un numero di radici che superi il suo grado.

99. Teorema 3.°—*Se* i *è una radice immaginaria della congruenza irriducibile*

$$f(x) \equiv 0 \pmod p$$

di grado ν, *i numeri complessi formati con* i *non che* i *reali* $1, 2, 3 \dots\dots p-1$ *saranno radici della congruenza*

$$x^{p^\nu - 1} - 1 \equiv 0 \pmod p.$$

Indichiamo con x_1 uno degl'indicati numori e formiamone le potenze successive: abbiamo così la serie indefinita

$$1, x_1, x_1^2, x_1^3, \ldots\ldots$$

nella quale debbono necessariamente essere comprese due potenze congrue secondo il modulo p, ossia tali che la loro differenza sia divisibile per $f(i)$, perchè $p^\nu-1$ sono i numeri reali o complessi incongrui secondo il modulo p e la funzione $f(i)$. Supponiamo che x_1^{m+n} sia la prima potenza per la quale si abbia

$$x_1^{m+n} \equiv x_1^m \pmod p,$$

ovvero
$$x_1^m(x_1^n - 1) \equiv 0 \pmod p,$$

ma $f(i)$, non dividendo x_1, non divide x_1^m, dunque dovrà essere

$$x_1^n - 1 \equiv 0 \pmod p.$$

Inoltre x_1^n è la minima potenza di x_1 che sia congrua ad 1, perchè se fosse

$$x_1^{n'} \equiv 1 \pmod p,$$

essendo $n' < n$, non sarebbe x_1^{m+n} la potenza più prossima ad x_1^m che fosse ad essa congrua. Di qui risulta che le potenze

$$1, x_1, x_1^2, \ldots\ldots x_1^{n-1} \qquad (1)$$

sono tutte distinte, per modo che se non esistesse un altro numero reale o complesso incongruo alla (1), sarebbe $n = p^\nu - 1$.

Ma supponiamo che vi sia un altro numero x_2 non congruo alle (1). Allora moltiplichiamo x_2 per ciascuna delle potenze (1) od abbiamo la serie

$$x_2, x_1^2x_2, x_1^3x_2, \ldots\ldots x_1^{n-1}x_2 \qquad (2)$$

nella quale nessun termine è congruo a zero, perchè ciascuno dei due fattori che compongono uno qualunque di essi non è divisibile por $f(i)$. Inoltre sono incongrui tra loro, perchè se fosse

$$x_2x_1^p \equiv x_2x_1^q \pmod p,$$

dovrebbe essere
$$x_1^p \equiv x_1^q \pmod p,$$

il che non è. Infine i medesimi numeri sono incongrui a quelli della serie (1), poichè se fosse

$$x_2x_1^p \equiv x_1^r \pmod p,$$

sarebbe
$$x_2x_1^n \equiv x_1^{n-p+r} \pmod p,$$

donde
$$x_2 \equiv x_1^{n-p+r} \pmod p,$$

il che è impossibile. Adunque se non vi fossero altri numeri incongrui a quelli contenuti nelle serie (1) e (2), sarebbe $p^\nu - 1 = 2n$. Ma se ve ne fosse un altro x_3, si dimostrerebbe come prima che i numeri

$$x_3, x_1^2x_3, x_1^3x_3 \ldots\ldots x_1^{n-1}x_3 \qquad (3)$$

sono incongrui tra loro ed a quelli delle serie (1) e (2), quindi se non vi fossero altri numeri incongrui a quelli contenuti nelle serie (1), (2), (3) sarebbe $p^\nu - 1 = 3n$. e così di seguito, per modo che n sarà un divisore di $p^\nu - 1$, ed $x_1^{p^\nu-1}$ sarà di-

visibile per $x_1^n - 1$, ma $x_1^n - 1$ è congruo a zero, dunque lo sarà anche $x_1^{p^\nu-1} - 1$, ed x_1 sarà radice della congruenza

$$x_1^{p^\nu-1} - 1 \equiv 0 \pmod{p}.$$

Corollario. — *La congruenza precedente ammette* $p^\nu - 1$ *radici.*

100. Si dice che un numero l reale o complesso appartenga all'esponente n, quando l^n è la più piccola potenza di l che sia congrua ad 1.

Dalla dimostrazione del precedente teorema risulta che, se l è una delle radici della precedente congruenza, debba essere n un divisore di $p^\nu - 1$.

Teorema 4.° — *Se* $\varphi(d)$ *dinota quanti sono i numeri minori di* d *che sono primi con esso, ad ogni divisore* d *di* $p^\nu - 1$, *corrispondono* $\varphi(d)$ *numeri reali o complessi.*

Supponiamo che x_1 sia un numero reale o complesso che corrisponda al divisore n di $p^\nu - 1$; allora i numeri

$$1, x_1, x_1^2, \ldots\ldots x_1^{n-1} \qquad (4)$$

saranno incongrui e le loro potenze n^{me} saranno congruo ad 1, per modo che i numeri (4) saranno radici della congruenza

$$x^n - 1 \equiv 0 \pmod{p},$$

ma questa congruenza non può avere più di n radici, dunque nella serie (4) bisogna trovare i numeri che corrispondono all'esponente n. Or supponiamo che x_1^m corrisponda a q, cosicchè si abbia

$$(x_1^m)^q \equiv 1 \pmod{p}$$

ovvero

$$x_1^{mq} \equiv 1 \pmod{p}.$$

ma x_1 corrisponde ad n, dunque mq è divisibile per n: laonde se indichiamo con δ il massimo comun divisore di m ed n, dovrà essere q divisibile per $\frac{n}{\delta}$, perciò il minimo valore che può assumere q è $\frac{n}{\delta}$, ma se m è primo con n, è $\delta = 1$ ed x_1^m corrisponde ad n, dunque o ad x_1 non corrisponde alcun esponente o ne corrisponderanno $\varphi(n)$; laonde se indichiamo con $\psi(n)$ la totalità dei numeri reali e complessi che corrispondono ad n, o sarà $\psi(n) = 0$ ovvero $\psi(n) = \varphi(n)$.

Dividiamo i $p^\nu - 1$ numeri reali e complessi non congrui tra loro in classi, riunendo quelli che appartengono allo stesso esponente, allora se osserviamo che uno di questi numeri non può appartenere che ad un solo divisore di $p^\nu - 1$, ed indichiamo con d_1, d_2, d_3 etc. i divisori di $p^\nu - 1$, avremo

$$\psi(d_1) + \psi(d_2) + \psi(d_3) + \ldots\ldots = p^\nu - 1,$$

ma si ha anche

$$\varphi(d_1) + \varphi(d_2) + \varphi(d_3) + \ldots\ldots = p^\nu - 1,$$

dunque sarà $\psi(d_1) + \psi(d_2) + \psi(d_3) + \ldots\ldots = \varphi(d_1) + \varphi(d_2) + \varphi(d_3) + \ldots\ldots$,

ma ciascun termine del 1° membro deve essere o zero ovvero uguale al termine corrispondente del 2°, dunque sarà generalmente

$$\psi(d) = \varphi(d).$$

Corollario. — *Vi sono* $\varphi(p^\nu - 1)$ *numeri che corrispondono a* $p^\nu - 1$.

Questi si chiamano radici primitive della congruenza

$$x^{p^\nu - 1} - 1 \equiv 0 \pmod{p}.$$

Similmente se n è un divisore di $p^\nu - 1$, i $\varphi(n)$ numeri che appartengono ad n si dicono radici primitive della congruenza

$$x^n - 1 \equiv 0 \pmod{p}.$$

101. Teorema 5.° — *Se* i *è una radice della congruenza irriducibile*

$$f(x) \equiv 0 \pmod{p}$$

di grado ν, *essa ammetterà le altre radici*

$$i^p, i^{p^2}, i^{p^3}, \ldots\ldots i^{p^{\nu-1}}.$$

Infatti sia $$f(i) = i^\nu + m i^{\nu-1} + \ldots\ldots$$

Innalziamo i due membri di quest'uguaglianza alle potenze p^r e sopprimiamo i multipli di p e si avrà

$$[f(i)]^{p^r} \equiv i^{\nu p^r} + m^{p^r} i^{(\nu-1)p^r} + \ldots\ldots \pmod{p},$$

ma, essendo m etc. numeri interi, pel teorema di Fermat, si ha

$$m^{p^\nu} \equiv m, \ldots\ldots,$$

quindi sarà $$[f(i)]^{p^r} \equiv i^{\nu p^r} + m i^{(\nu-1)p^r} + \ldots\ldots = f(i^{p^r}),$$

ma $$[f(i)]^{p^r} \equiv 0 \pmod{p},$$

dunque sarà anche $$f(i^{p^r}) \equiv 0 \pmod{p},$$

qualunque sia r.

Ora le ν radici $i, i^p, i^{p^2} \ldots\ldots i^{p^{\nu-1}}$ sono incongrue. Poichè se si avesse

$$i^{p^r} \equiv i^{p^\rho} \pmod{p},$$

essendo $\rho < r < \nu$, sarebbe

$$(a i^{\nu-1} + b i^{\nu-2} + \ldots)^{p^r} \equiv a i^{(\nu-1)p^r} + b i^{(\nu-2)p^r} + \ldots \equiv a i^{(\nu-1)p^\rho} + b i^{(\nu-2)p^\rho} + \ldots$$
$$\equiv (a i^{\nu-1} + b i^{\nu-2} + \ldots)^{p^\rho}$$

quindi i $p^\nu - 1$ numeri radici della congruenza

$$x^{p^\nu - 1} \equiv 1 \pmod{p}$$

sarebbero anche radici dell'altra

$$x^{p^{r-\rho}} \equiv x \pmod{p}$$

il che è impossibile perchè $p^{r-\rho}$ è minore di $p^\nu - 1$.

Osservazioni—Se $\varphi(i)$ è una funzione qualunque di i, le funzioni $\varphi(i), \varphi(i^p), \ldots, \varphi(\varphi^{p^{\nu-1}}($ si dicono conjugate l'une dell'altre

Or se un intero complesso $\varphi(i)$ sodisfa ad una congruenza $F(x) \equiv 0$ i suoi conjugati vi sodisfano ugualmente.

Infatti per essere $F[\varphi(i)] \equiv 0$ è necessario che $F[\varphi(x)]$ sia divisibile per $f(x)$, ed allora tutte le radici di $f(x) \equiv 0$ l'annulleranno e sarà $F[\varphi(i^p)] \equiv 0$ etc.

102. Teorema 6.° — *Qualunque sia il numero ν esiste sempre una funzione irriducibile di grado ν.*

Indichiamo con $\varphi(x)$, $\varphi'(x)$ etc. i fattori irriducibili in cui si può scomporre la funzione

$$Y = x^{p^\nu} - x.$$

È evidente che le radici delle congruenze

$$\varphi(x) \equiv 0 \pmod p, \quad \varphi'(x) \equiv 0 \pmod p \ldots$$

siano appunto le radici della congruenza

$$x^{p^\nu} - x \equiv \pmod p.$$

Supponiamo che λ sia il grado della congruenza

$$\varphi(x) \equiv 0 \pmod p$$

e che l sia una delle sue radici, allora sarà

$$l^{p^\lambda} \equiv l, \quad l^{p^{\lambda+1}} \equiv l^p, \quad l^{p^{\lambda+2}} \equiv l^{p^2} \ldots,$$

quindi nella serie $\qquad l, \; l^p, \; l^{p^2}, \; l^{p^3} \ldots$

i soli termini $\qquad l^{p^\lambda}, \; l^{p^{2\lambda}}, \; l^{p^{3\lambda}} \ldots$

saranno congrui ad l, ma si ha $\qquad l^{p^\nu} \equiv l.$

dunque λ divide ν.

Ora supponiamo che sia $\nu = q^\alpha$, essendo q un numero primo. Se λ è minore di ν dovrà dividere $q^{\alpha-1}$, ed l sarà la radice della congruenza

$$x^{p^{q^{\alpha-1}}} \equiv x \pmod p,$$

che perciò la funzione $X = x^{p^{q^{\alpha-1}}} - x$ sarà divisibile per $\varphi(x)$ e per tutti gli altri fattori $\varphi'(x)$, $\varphi''(x)$ etc. i cui gradi sono inferiori a ν, ma tutti questi fattori sono disuguali, perchè tra $x^{p^\nu} - x$ e la sua prima derivata -1 non vi è massimo comun divisore; dunque $x^{p^{q^{\alpha-1}}} - x$ dovrà essere uguale al prodotto di tutt'i fattori $\varphi(x)$, $\varphi'(x)$, $\varphi''(x)$ etc. i cui gradi sono minori di ν, e per conseguenza il quoziente $\frac{Y}{X}$ di grado $q^\alpha - q^{\alpha-1}$ sarà uguale al prodotto dei fattori di grado ν, il cui numero sarà indicato da $\frac{q^\alpha - q^{\alpha-1}}{\nu}$.

Supponiamo che sia $\nu = q^\alpha r^\beta s^\gamma \ldots$ Siano $j, j', j'' \ldots$ radici di congruenze di gradi $q^\alpha, r^\beta, s^\gamma$ etc., si avrà

$$j^{p^{q^\alpha}} \equiv j, \quad j'^{p^{r^\beta}} \equiv j', \quad j''^{p^{s^\gamma}} \equiv j'' \ldots,$$

ma ν è divisibile per q^α, r^β, s^γ etc., dunque sarà

$$j^{p^\nu} \equiv j, \quad j'^{p^\nu} \equiv j', \quad j''^{p^\nu} \equiv j'' \ldots$$

donde $\qquad (j j' j'' \ldots)^{p^\nu} \equiv j j' j'' \ldots$

ed $jj'j''\ldots$ sarà radice della congruenza

$$x^{p^\nu} - x \equiv 0 \pmod p$$

e per conseguenza radice di una delle congruenze

$$\varphi(x) \equiv 0, \quad \varphi'(x) \equiv 0, \quad \varphi''(x) \equiv 0 \ldots \pmod p.$$

Supponiamo che appartenga alla 1ª di queste congruenze che è di grado λ. Se λ è minore di ν, dovrà dividere uno dei numeri $\frac{\nu}{q}$, $\frac{\nu}{r}$, $\frac{\nu}{s}$ etc. Poniamo che divida $\frac{\nu}{q}$, allora sarà

$$(jj'j''\ldots)^{p^{\frac{\nu}{q}}} \equiv jj'j''\ldots,$$

ma

$$j'^{p^{\frac{\nu}{q}}} \equiv j', \quad j''^{p^{\frac{\nu}{q}}} \equiv j'' \ldots,$$

dunque sarà

$$j^{p^{\frac{\nu}{q}}} \equiv j,$$

il che è impossibile, perchè $\frac{\nu}{q}$ non è divisibile per q^α, per conseguenza è anche impossibile che λ sia minore di ν.

102. Teorema 7.° — *Se μ', μ'', μ''' etc. sono i gradi dei fattori irriducibili in cui si può scomporre la funzione intera* F(x), *e se s'indica con $\nu = \mu d$ il minimo multiplo di μ', μ'', μ''' etc., la congruenza*

$$F(x) \equiv 0 \pmod p$$

avrà $\mu' + \mu'' + \mu''' + \ldots$ radici che saranno funzioni intere di una radice immaginaria i di una congruenza irriducibile di grado ν.

Infatti se indichiamo con $f(x)$, $f'(x)$ etc. i fattori irriducibili di $F(x)$, le radici delle congruenze proposte saranno appunto quelle dell'altre

$$f(x) \equiv 0, \quad f'(x) \equiv 0 \ldots \pmod p$$

le quali ammettono rispettivamente μ, μ', μ'' etc. radici.

Ora indichiamo con j una radice della congruenza

$$f(x) \equiv 0 \pmod p$$

chè è di grado μ, si avrà

$$j^{p^\mu} \equiv j$$

e quindi

$$j^{p^\nu} \equiv j^{p^\mu \cdot p^{\mu(d-1)}} \equiv j^{p^{\mu(d-1)}} \equiv j^{\mu(d-2)} \equiv \ldots \equiv j,$$

laonde le μ radici di

$$f(x) \equiv 0 \pmod p$$

saranno altresì radici di

$$x^{p^\nu - 1} - 1 \equiv 0 \pmod p,$$

ma se i è una radice immaginaria di questa congruenza, tutte l'altre sono funzioni intere di i, dunque le radici di

$$f(x) \equiv 0 \pmod p$$

sono funzioni intere di i. Lo stesso discorso è applicabile a ciascuna dell'altre congruenze.

$$f'(x) \equiv 0, \quad f''(x) \equiv 0 \ldots \pmod p.$$

COROLLARIO — Se indichiamo con $x_1, x_2 \ldots x_m$ le radici delle congruenze

$$F(x) \equiv 0 \pmod{p} \qquad (a)$$

di grado m, e che abbia per coefficiente del 1° termine 1, sarà

$$F(x) = (x - x_1)(x - x_2) \ldots (x - x_m) + f(i)\,\varphi(x, i) + p\varphi_1(x, i),$$

ma $$f(i) \equiv 0 \pmod{p}$$

dunque sarà $$F(x) \equiv (x - x_1)(x - x_2) \ldots (x - x_m) \pmod{p}$$

ponde si rileva: *Che tra i coefficienti di* F(x) *e le radici della congruenza* (a) *esistono le stesse relazioni che vi sono tra i coefficienti del 1° membro di un' equazione ordinata e le sue radici, solo che l'uguaglianze debbono mutarsi in congruenze.*

CAPO 2.°

Residui quadratici.

104. Essendo $p-1$ un divisore di $p^\nu-1$ saranno $\varphi(p-1)$ i numeri che corrisponderanno all'esponente $p-1$. Questi saranno reali, perchè debbono sodisfare alla congruenza

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

la quale non ammette radici immaginarie in forza del teorema di Fermat. Quindi se indichiamo con g uno di tali numeri, i termini della serie

$$1,\ g,\ g^2, \ldots\ldots g^{p-1},$$

presi con altro ordine, saranno identici a quelli dell'altra

$$1,\ 2,\ 3 \ldots\ldots p-1.$$

TEOREMA 1.° — *Se* δ *indica il massimo comun divisore tra* $n < p-1$ e $p-1$, *la congruenza*

$$x^n \equiv D \pmod{p}, \qquad (1)$$

in cui D *dinota un numero reale ed intero, avrà* δ *radici reali o non ne avrà alcuna, secondochè avrà luogo o non avrà luogo la congruenza*

$$D^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}. \qquad (2)$$

Sia x' una radice reale della congruenza (1), ed abbiasi

$$x' \equiv g^{\gamma'}, \quad D \equiv g^{\gamma} \pmod{p},$$

allora dovrà essere $$g^{n\gamma'} \equiv g^{\gamma} \pmod{p}, \qquad (3)$$

ma nella serie $$1,\ g,\ g^2 \ldots g^{p-1},\ g^p,\ g^{p+1} \ldots$$

due termini sono tra loro congrui, quando la differenza dei loro esponenti è divisibile per $p-1$, ossia quando questi esponenti sono congrui secondo il modulo $p-1$, dunque dovrà essere

$$n\gamma' \equiv \gamma \pmod{p-1}; \qquad (4)$$

e reciprocamente se ha luogo quest' ultima congruenza reggerà anche la (3), ma la congruenza (4) non può esser verificata per alcun valore di γ' se n e $p-1$ hanno

un massimo comun divisore δ che non divide γ, e lo è per δ valori di γ' nel caso contrario, dunque la (1) o non ammetterà alcuna radice reale o ne ammetterà δ, secondochè δ non divide o divide γ. Ma se ha luogo la (2), ponendovi g^γ in luogo di D, si ha

$$g^{\gamma\frac{p-1}{\delta}} \equiv 1 \pmod{p},$$

e quindi γ sarà divisibile per δ, e quante volte γ non è divisibile per δ non può esistere la (2), dunque resta dimostrata la proposizione enunciata.

Corollario — Di qui segue che la congruenza

$$x^2 \equiv D \pmod{p}$$

ammetterà radici reali quando si ha

$$D^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Ma il massimo comun divisore tra $p-1$ e $\frac{p-1}{2}$ è $\frac{p-1}{2}$, e si ha

$$1^2 \equiv 1 \pmod{p},$$

dunque *vi saranno* $\frac{p-1}{2}$ *numeri* D *minori di* p *pei quali la congruenza*

$$x^2 \equiv D \pmod{p}$$

ammetterà radici reali.

Questi numeri si dicono resti quadratici di p ed i rimanenti dei $p-1$ numeri minori di p si dicono non resti quadratici o semplicemente non resti di p.

105. Teorema 2.° — *Il prodotto* abc... *sarà residuo quadratico* o *non residuo quadratico secondochè è pari o impari il numero dei fattori che non sono residui.*

Pel teorema di Fermat si ha, qualunque sia il numero D,

$$D^{p-1} \equiv 1 \pmod{p}$$

ovvero

$$\left(D^{\frac{p-1}{2}} - 1\right)\left(D^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p},$$

ma se D non è residuo $D^{\frac{p-1}{2}} - 1$, non è divisibile per p, dunque in questo caso dovrà essere

$$D^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

ma si ha

$$(abc\ldots)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \cdot c^{\frac{p-1}{2}} \ldots,$$

dunque $(abc\ldots)^{\frac{p-1}{2}}$ sarà congruo ad 1 o a -1, secondochè è pari o impari il numero dei fattori del 2° membro che sono congrui a -1.

Legendre ha indicato col simbolo $\left(\frac{m}{p}\right)$ l'unità o meno l'unità, secondochè il numero m, non divisibile per p, è residuo o non residuo. Usando di questa notazione, il teorema precedente può esprimersi nel seguente modo

$$\left(\frac{abc\ldots}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)\ldots\ldots$$

CAPO 3.°

Congruenze di 2° grado a più ignote.

106. Sia da risolversi la congruenza

$$a_1x_1^2 + a_2x_2^2 \equiv k \pmod p.$$

Poniamo
$$a_1x_1 \equiv y \pmod p, \tag{1}$$
allora la proposta congruenza prenderà la forma
$$y^2 + a_1a_2x_2^2 \equiv a_1k \pmod p. \tag{2}$$

Supponiamo dapprima che $-a_1a_2$ sia residuo quadratico di p e che λ sia un numero tale che si abbia
$$\lambda^2 \equiv -a_1a_2 \pmod p.$$
Sostituendo λ^2 a $-a_1a_2$, la (2) prenderà la forma
$$y^2 - \lambda^2x_2^2 \equiv a_1k \pmod p,$$
e ponendo
$$y - \lambda x_2 \equiv v, \quad y + \lambda x_2 \equiv u \tag{3}$$
si avrà
$$vu \equiv a_1k \pmod p. \tag{4}$$

Se k è diverso da zero possiamo dare ad u uno dei seguenti valori $1, 2, 3 \ldots p-1$, indi dalla (4) si ricaverebbe il valore di v, dalle (3) i valori di y e di x_2, ed infine dalla (1) il valore di x_1; quindi in questo caso vi sarebbero $p-1$ sistemi di valori di x_1 e di x_2.

Se $k \equiv 0$ possiamo dare ad u il valore 0 ed a v uno qualunque dei seguenti $1, 2, 3 \ldots p-1$, o viceversa; quindi in questo caso vi saranno $2(p-1)$ soluzioni.

Supponiamo in secondo luogo che $-a_1a_2$ non sia residuo quadratico; allora la funzione $x^2 + a_1a_2$ sarà irriducibile, perchè se fosse
$$x^2 + a_1a_2 = (x - h)(x - h_1) + pf(x),$$
h^2 ed h_1^2 divisi per p darebbero per residuo $-a_1a_2$, il che è contrario all'ipotesi.

Indichiamo con i una delle radici immaginarie della congruenza irriducibile
$$x^2 + a_1a_2 \equiv 0 \pmod p)$$
l'altra sarà $-i \equiv i^p$.

Ora essendo
$$i^2 + a_1a_2 \equiv 0 \pmod p$$
e quindi
$$i^2x_2^2 + a_1a_2x_2^2 \equiv 0 \pmod p,$$
la (2) può mettersi sotto la forma
$$y^2 + a_1a_2x_2^2 - i^2x_2^2 - a_1a_2x_2^2 - a_1k \equiv 0 \pmod p,$$
ovvero
$$y^2 - i^2x_2^2 - a_1k \equiv 0 \pmod p,$$
ma
$$y^2 - i^2x_2^2 = (y + ix_2)(y - ix_2) \equiv (y + ix_2)(y + i^px_2) \equiv (y + ix_2)^{p+1},$$
dunque sarà
$$(y + ix_2)^{p+1} - a_1k \equiv 0 \pmod p,$$
e ponendo
$$y + ix_2 \equiv z,$$
sarà
$$z^{p+1} - a_1k \equiv 0 \pmod p. \tag{5}$$

Indichiamo con u una radice primitiva della congruenza

$$x^{p^2} - x \equiv 0 \pmod p,$$

e poniamo $a_1 k \equiv u^\beta$;

allora sarà $u^{\beta(p-1)} \equiv (a_1 k)^{p-1} \equiv 1$

donde $\beta (p-1) \equiv 0 \pmod{p^2 - 1}$

e quindi $\beta = m (p+1)$,

essendo m un numero intero.

Inoltre poniamo $z \equiv u^t$

e sostituiamo i valori di z e di $a_1 k$ nella (5), ed abbiamo

$$u^{t(p+1)} - u^{m(p+1)} \equiv 0 \pmod p$$

donde la congruenza $t(p+1) \equiv m(p+1) \pmod{p^2 - 1}$

la quale ha le seguenti radici

$$m,\ \ m+p-1,\ \ m+2(p-1), \ldots$$

di cui $p+1$ sono incongrue secondo il modulo $p^2 - 1$. Or supponiamo che uno di questi valori di t si sia posto nell'espressione u^t, sopprimendo nel risultato le parti divisibili per $i^2 + a_1 a_2$ e per p, si avrà un'espressione della forma $a + bi$, ed uguagliando secondo il modulo p a ad y o b ad x_2, si avranno i valori di y o di x_2 corrispondenti al valore di t che si considera; indi si troverà il valore di x, mediante la (1): adunque nel caso che si considera la proposta congruenza ammetterà $p+1$ soluzioni.

107. Teorema 1.° — *Secondochè* -1 *è residuo quadratico o non residuo quadratico di* p *il numero dei residui seguiti da residui nella serie* 1, 2, 3 ... p − 1 *sarà* $\frac{p-1}{4} - 1$ *ovvero* $\frac{p-3}{4}$, *e quello dei residui seguiti da non residui sarà* $\frac{p-1}{4}$ *ovvero* $\frac{p+1}{4}$.

Infatti la congruenza $y^2 \equiv x^2 + 1 \pmod p$

ha $p-1$ soluzioni le quali sono di tre specie: 1° Quelle in cui $x \equiv 0$ ed $y \equiv \pm 1$ che sono due: 2° Quelle in cui $x^2 \equiv a$ od $y^2 \equiv a+1$, essendo a un residuo seguito da un residuo, il cui numero sarà 4φ, se indichiamo con φ il numero dei valori di a, poichè essendo ambigui i segni d'x e d'y, ad ogni valore di a corrisponderanno due valori per x ed altrettanti per y: 3° Quelle in cui $y \equiv 0$ ed $x^2 + 1 \equiv 0$, quando -1 è residuo quadratico, le quali sono due.

Supponiamo in prima che -1 sia residuo quadratico di p. Il numero delle soluzioni di

$$y^2 \equiv x^2 + 1 \pmod p$$

sarà $2 + 4\varphi + 2 = p + 1$

donde $\varphi = \frac{p-1}{4} - 1$.

Ma il numero dei residui contenuti nelle serie $1, 2, \ldots p-1$ è $\frac{p-1}{2}$, e l'ul-

timo $p-1$ non è seguito da altri, dunque il numero dei residui seguiti da non residui sarà

$$\frac{p-1}{2}-1-\frac{p-1}{4}+1=\frac{p-1}{4}.$$

Supponiamo che -1 non sia residuo. Allora sarà

$$2+4\varphi=p-1$$

donde
$$\varphi=\frac{p-3}{4},$$

ed il numero dei residui seguiti da non residui sarà

$$\frac{p-1}{2}-\frac{p-3}{4}=\frac{p+1}{4}.$$

108. Teorema 2.° — *Il numero dei sistemi di soluzioni della congruenza*

$$a_1 x_1^2 + a_2 x_2^2 + \ldots + a_{2n} x_{2n}^2 \equiv k \pmod p \qquad (1)$$

in cui $a_1, a_2 \ldots a_{2n}$ *sono* $\gtrless 0 \pmod p$ *è uguale a* $p^{2n-1}-p^{n-1}\nu$ *ovvero a* $p^{2n-1}+(p^n-p^{n-1})\nu$, *secondochè si ha* $k \gtrless 0$ *ovvero* $k\equiv 0 \pmod p$, *dinotando* ν *il simbolo* $\left(\frac{(-1)^n a_1 a_2 \ldots a_{2n}}{p}\right)$.

Pel teorema testè dimostrato si vede che la precedente proposizione è vera pel caso di $n=1$; quindi essa sarà sempre vera se verificandosi per $n=l$ ed $n=m$ si verifica anche per $n=m+l$.

Indichiamo con y un'indeterminata, e supponiamo che la proposizione sia vera per le due congruenze

$$a_1 x_1^2 + a_2 x_2^2 + \ldots + a_{2l} x_{2l}^2 \equiv y \qquad (2)$$

$$a_{2l+1} x_{2l+1}^2 + \ldots + a_{2(l+m)} x_{2(l+m)}^2 \equiv k-y \qquad (3)$$

equivalenti alla (1).

Sia primieramente $k \gtrless 0 \pmod p$. Per ogni valore di y differente da 0 e da $k \pmod p$ la (2) ha per ipotesi $p^{2l-1}-p^{l-1}\lambda$ soluzioni, e la (3) ne ha $p^{2m-1}-p^{m-1}\mu$, essendo

$$\lambda=\left(\frac{(-1)^l a_1 a_2 \ldots a_{2l}}{p}\right), \qquad \mu\left(\frac{(-1)^m a_{2l+1} \ldots a_{2(l+m)}}{p}\right).$$

Per $y\equiv 0$ esse hanno rispettivamente $(p^{2l-1}+(p^l-p^{l-1})\lambda$ e $p^{2m-1}-p^{m-1}\mu$ soluzioni. Infine per $y=k$ esse hanno $p^{2l-1}-p^{l-1}$ e $p^{2m-1}+(p^m-p^{m-1})\mu$ soluzioni. Adunque il numero totale delle soluzioni sarà

$$(p-2)(p^{2l-1}-p^{l-1}\lambda)(p^{2m-1}-p^{m-1}\mu)+(p^{2l-1}-p^{l-1}\lambda)[p^{2m-1}+(p^m-p^{m-1})\mu]$$
$$+(p^{2m-1}-p^{m-1}\mu)(p^{2l-1}+(p^l-p^{l-1})\lambda]=p^{2l+2m-1}-p^{l+m-1}\lambda\mu,$$

e sostituendo ν in luogo di $\lambda\mu$, si avrà la formola indicata nell'enunciato.

Sia in secondo luogo $k\equiv 0$. Ponendo prima $y \gtrless 0$ ed indi $y\equiv 0$ e sommando i numeri delle soluzioni corrispondenti a quest'ipotesi si ha

$$(p-1)(p^{2l-1}-p^{l-1}\lambda)(p^{2m-1}-p^{m-1}\mu)+[p^{2l-1}+(p^l-p^{l-1})\lambda][p^{2m-1}+(p^m-p^{m-1})\mu]$$
$$=p^{2(l+m)-1}+(p^{l+m}-p^{l+m-1})\lambda\mu=p^{2(l+m-1)}+(p^{l+m}-p^{l+m-1})\nu.$$

109. Teorema 3.° – *Il numero dei sistemi di soluzioni della congruenza*

$$a_1 x_1^2 + a_2 x_2^2 + \dots + a_{2n+1} x^2_{2n+1} \equiv k \pmod p \qquad (4)$$

è $p^{2n} - p^n v'$, *ponendo per brevità* $v' = \left(\frac{(-1)^n a_1 a_2 \dots a_{2n+1} k}{p}\right)$.

La congruenza proposta equivale alle due seguenti

$$a_1 x_1^2 \equiv y$$

$$a_2 x_2^2 + \dots + a_{2n+1} x^2_{2n+1} \equiv k - y \qquad (5)$$

la prima delle quali si può mettere sotto la forma

$$a_1^2 x_1^2 \equiv a_1 \cdot y. \qquad (6)$$

Supponiamo che sia $\mu = \left(\frac{a_1 k}{p}\right) \equiv 0 \pmod p$. Allora tanto è dare alla y nella (6) il valore zero quanto l'altro k. Questa congruenza per $y=0$ dà $x_1=0$, per un valore di y che rende $a_1 y$ un residuo quadratico r^2 dà $x_1 = \pm \frac{r}{a_1}$, e per ogni valore di y che non rende $a_1 y$ residuo quadratico è impossibile. Ma per $y=k$ la (5) dà

$$p^{2n-1} + (p^n - p^{n-1}) v$$

soluzioni, e per ogni valore di y diverso da k ne dà

$$p^{2n-1} - p^{n-1} v,$$

dunque, essendo $\frac{p-1}{2}$ il numero dei valori di y che rendono $a_1 y$ residuo quadratico, il numero delle soluzioni della (4) sarà

$$p^{2n-1} + (p^n - p^{n-1}) v + 2 (p^{2n-1} - p^{n-1} v) \frac{p-1}{2}. \qquad (7)$$

Sia $\left(\frac{a_1 k}{p}\right) = 1$. Allora per $y=0$ la (6) dà una soluzione e la (5) $p^{2n-1} - p^{n-1} v$; per $y=k$ la (6) ne dà due e la (5)

$$p^{2n-1} + (p^n - p^{n-1}) v;$$

ed infine per ogni valore di y, diverso da k, che rende $a_1 y$ residuo quadratico la (6) ne dà due e la (5)

$$p^{2n-1} - p^{n-1} v,$$

ma questi ultimi valori di y sono $\frac{p-1}{2} - 1$, dunque il numero delle soluzioni della (4) sarà

$$p^{2n-1} - p^{n-1} v + 2 \left[p^{2n-1} + \left(p^n - p^{n-1}\right) v\right] + 2 \left(\frac{p-1}{2} - 1\right) \left(p^{2n-1} - p^{n-1} v\right). \qquad (8)$$

Sia $\left(\frac{a_1 k}{p}\right) = -1$. In questo caso per $y=k$ la (6) è impossibile, quindi il numero delle soluzioni della (4) sarà

$$p^{2n-1} - p^{n-1} v + 2 \frac{p-1}{2} (p^{2n-1} - p^{n-1} v). \qquad (9)$$

L'espressioni (7), (8), (9) si riducono rispettivamente alle altre

$$p^{2n}, \quad p^{2n} + p^n v, \quad p^{2n} - p^n v$$

per le quali μ ha rispettivamente i valori, 0, 1, -1, ma $\mu v = v'$, dunque quest'espressioni si comprendono nella seguente formola

$$p^{2n} + p^n v'.$$

PARTE TERZA (*)

SOSTITUZIONI LINEARI.

CAPO 1.°

Rappresentazione analitica delle Sostituzioni.

110. Se rappresentiamo m grandezze con una sola lettera l affetta da un indice x variabile da 0 ad $m-1$, e dinotiamo con

$$a_0, a_1, \dots a_{m-1}; \quad b_0, b_1, \dots b_{m-1}$$

i numeri 0, 1, 2, ... $m-1$ disposti con due ordini diversi, la sostituzione S che scambia le lettere che hanno per indici $a_0, a_1, \dots a_{m-1}$ rispettivamente con quelle che hanno per indici $b_0, b_1, \dots b_{m-1}$ può essere rappresentata dal simbolo

$$S = [x, \varphi(x)]$$

in cui $\varphi(x)$ indica una funzione che prende i valori $b_0, b_1, \dots b_{m-1}$ quando si fa la x successivamente uguale ad $a_0, a_1, \dots a_{m-1}$.

La formola d'interpolazione di Lagrange dà per $\varphi(x)$ il seguente valore

$$\varphi(x) = \frac{b_0 f(x)}{(x-a_0) f'(x)} + \frac{b_1 f(x)}{(x-a_1) f'(x)} + \dots + \frac{b_{m-1} f(x)}{(x-a_{m-1}) f'(x)},$$

essendo $$f(x) = (x-a_0)(x-a_1)\dots(x-a_{m-1})$$

ed $f'(x)$ la derivata di $f(x)$.

(*) Il materiale di questa terza parte è stato dedotto dal Trattato delle Sostituzioni del Sig. Jordan.

Se conveniamo che la quantità rappresentata da l_x lo sia anche da l_y, essendo y un numero congruo ad x secondo il modulo m, la sostituzione S può essere rappresentata dal simbolo

$$S = [x, \varphi(x)] \pmod{m},$$

essendo $\varphi(x)$ una funzione che dà dei risultati congrui a $b_0, b_1, \dots b_{m-1}$ quando alla x si danno i valori $a_0, a_1, \dots a_{m-1}$, ovvero altri congrui ai precedenti secondo il modulo m.

Di qui risulta che la condizione a cui deve soddisfare una funzione $\varphi(x)$ per potere esprimere una sostituzione di m quantità è che ad m valori della x incongrui secondo il modulo m corrispondano per la funzione m valori disuguali ed incongrui secondo il medesimo modulo. Quando m è un numero primo, il carattere distintivo delle funzioni che godono di questa proprietà è dato dal seguente teorema dovuto ad Hermite.

111. Teorema. — *Affinchè una funzione intera di* x *a coefficienti interi possa rappresentare una sostituzione di* p *indici incongrui secondo il modulo primo* p, *è necessario e sufficiente che siano congrui a zero i coefficienti di* x^{p-1} *nelle prime* $p-2$ *potenze di questa funzione, ridotte mediante la congruenza*

$$x^p \equiv x \pmod{p}.$$

Supponiamo che $[x, f(x)]$ rappresenti una sostituzione di p indici, e che dopo aver ridotta $f(x)$ mediante la congruenza

$$x^p \equiv x \pmod{p}$$

si sia ottenuto

$$f(x) \equiv A_0 + A_1 x + A_2 x^2 + \dots + A_{p-1} x^{p-1} \pmod{p}.$$

Poniamo

$$\varphi(x) = A_0 + A_1 x + A_2 x^2 + \dots + A_{p-1} x^{p-1}$$

$$[\varphi(x)]^m \equiv A_0^{(m)} + A_1^{(m)} x + A_2^{(m)} x^2 + \dots + A_{p-1}^{(m)} x^{p-1} \pmod{p}.$$

Sostituiamo in quest'ultima congruenza $0, 1, 2 \dots p-1$ in luogo di x ed addizioniamo i risultati, si avrà

$$\Sigma [\varphi(x)]^m \equiv p A_0^{(m)} + A_1^{(m)} \Sigma x + A_2^{(m)} \Sigma x^2 + \dots + A_{p-1}^{(m)} \Sigma x^{p-1} \pmod{p}.$$

Or poichè le radici della congruenza

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

sono $1, 2, 3 \dots p-1$, per le relazioni di Newton si ha che la somma

$$S_m = 1^m + 2^m + 3^m + \dots + (p-1)^m$$

è congrua a zero per tutt'i valori di m inferiori a $p-1$. Ma x^{p-1} è congruo a zero per $x = 0$ e ad 1 per ogni altro valore della x, quindi sarà

$$\Sigma x \equiv 0, \quad \Sigma x^2 \equiv 0, \dots \Sigma x^{p-2} \equiv 0, \quad \Sigma x^{p-1} \equiv p-1,$$

e per conseguenza

$$\Sigma [\varphi(u)]^m \equiv -A_{p-1}^{(m)} \pmod{p};$$

ma per tutt'i valori di m minori di $p-1$ si ha

$$\Sigma[\varphi(x)]^m = \Sigma[\varphi(0)^m + \varphi(1)^m + \ldots + \varphi(p-1)^m] \equiv [1^m + 2^m + \ldots + (p-1)^m] \equiv 0 \pmod p$$

dunque per i medesimi valori di m si ha

$$A^{(m)}_{p-1} \equiv 0 \pmod p.$$

Viceversa supponiamo che la precedente congruenza si verifichi per tutt'i valori di m inferiori a $p-1$; allora $\Sigma[\varphi(x)]^m$ sarà congrua a zero per gli stessi valori di m, ed è anche congrua a zero per $m=p$, perchè essendo

$$x^p \equiv x \pmod p$$

sarà $\quad \varphi(0)^p + \varphi(1)^p + \ldots + \varphi(p-1)^p \equiv 1 + 2 + \ldots + p - 1 \equiv 0 \pmod p,$

quindi per le relazioni di Newton la congruenza

$$[z-\varphi(0)][z-\varphi(1)] \ldots [z-\varphi(p-1)] \equiv 0 \pmod p$$

dovrà avere la forma $\quad z^p - \alpha z \equiv 0 \pmod p,$

ma si ha $\quad z^p - z \equiv 0 \pmod p,$

dunque sarà $\quad (\alpha - 1) z \equiv 0 \pmod p.$

Ora se α fosse diversa da 1, quest'ultima congruenza non potrebbe essere sodisfatta che da $z=0$, e quindi le p quantità $\varphi(0), \varphi(1), \ldots \varphi(p-1)$ dovrebbero essere uguali a zero, il che è impossibile, perchè $\varphi(x)$ è di grado $p-1$, quindi dovrà essere $\alpha = 1$. Di qui risulta che $\varphi(0), \varphi(1) \ldots \varphi(p-1)$ debbano essere radici della congruenza

$$z^p - z \equiv 0 \pmod p$$

perciò congrue a $0, 1, 2, \ldots p-1$, e per conseguenza $f(x)$ potrà rappresentare una sostituzione.

112. Si sa che quante volte α è primo con p, l'espressione $\alpha x + \beta$ dà una serie completa di numeri incongrui secondo il modulo p, quando ad x si danno successivamente p valori disuguali ed incongrui secondo lo stesso modulo, quindi se $f(x)$ può rappresentare una sostituzione, anche l'altra

$$f_1(x) = \alpha f(x+\beta) + \gamma$$

può essere adoperata per questo ufficio. E poichè α, β, γ sono tre costanti arbitrarie, possiamo determinare α colla condizione che il coefficiente della più alta potenza di x sia l'unità, β colla condizione che si annulli il coefficiente del 2° termine, e γ colla condizione che si annulli l'ultimo termine, allora $f_1(x)$ prenderà la seguente forma

$$f_1(x) = a_1 x + a_2 x^2 + \ldots + a_{\nu-2} x^{\nu-2} + x^\nu$$

essendo ν uguale o minore di $p-1$.

Alle funzioni $f_1(x)$ Hermite ha dato il nome di funzioni ridotte. È chiaro che

ogni funzione ridotta $f_1(x)$ dia una funzione più generale

$$\alpha f_1(x+\beta)+\gamma$$

in cui α, β, γ sono quantità indeterminate.

113. Se il numero m delle quantità è uguale alla potenza n^{ma} di un numero primo p, rappresenteremo ciascuna di esse con una medesima lettera affetta da n indici x, x', x'' etc. variabili da 0 a $p-1 \pmod p$ ed una sostituzione che scambia x, x', x'' etc. rispettivamente in

$$\varphi(x, x', x''...), \quad \psi(x, x', x''...), \quad \chi(x, x', x''...), \; ...$$

col simbolo

$$[x, x', x''... \quad \varphi(x, x', x''...), \quad \psi(x, x', x''...), \quad \chi(x, x', x''...)...]$$

essendo ciascuna delle funzioni $\varphi(x, x', x''...)$ etc. di un grado uguale o minore di $p-1$ per rispetto a ciascun indice.

Questo metodo potrebbe anche essere esteso al caso in cui il numero m delle quantità fosse il prodotto di più numeri primi diversi, ma si andrebbe incontro a grande complicazione.

CAPO 2.°

Generalità sulle sostituzioni lineari.

114. Teorema 1.°—*Siano* m *ed* n *due numeri interi qualunque ed* $l_{x,x'}, \ldots,$ $l_{x'',x'}, \ldots, \ldots$ m^n *simboli distinti per mezzo di* n *indici variabili da* 0 *ad* $m-1$ (mod m). *Affinchè l'espressione*

$$S=[x, x', x'', \ldots\; ax+bx'+cx''+\ldots, \; a'x+b'x'+c'x''+\ldots, \; a''x+b''x'+c''x''+\ldots, \ldots]$$

possa rappresentare una sostituzione è necessario e sufficiente che il determinante di S

$$\Delta=\begin{vmatrix} a & b & c \; \ldots \\ a' & b' & c' \; \ldots \\ a'' & b'' & c'' \ldots \\ \cdot & \cdot & \cdot \; \cdot \; \cdot \end{vmatrix}$$

sia primo con m.

Questa condizione è sufficiente; poichè, dinotando con x_1, x_2 etc. delle quantità incongrue secondo il modulo m, possiamo trovare per x, x', x'' etc. dei valori incongrui secondo lo stesso modulo che sodisfano alle congruenze

$$(1) \qquad \Delta x \equiv \frac{d\Delta}{da}x_1+\frac{d\Delta}{da'}x_2+\ldots, \; \Delta x' \equiv \frac{d\Delta}{db}x_1+\frac{d\Delta}{db'}x_2+\ldots,$$

$$\Delta x'' \equiv \frac{d\Delta}{dc}x_1+\frac{d\Delta}{dc'}x_2+\ldots, \ldots \pmod m$$

ma queste congruenze sono equivalenti all'altre

$$ax+bx'+cx''+\ldots \equiv x_1, \quad a'x+b'x'+c'x''+\ldots \equiv x_2, \quad a''x+b''x'+c''x''+\ldots \equiv x_3, \ldots \pmod m,$$

quindi l'espressioni

$$ax+bx'+cx''+\dots,\quad a'x+b'x'+c'x''+\dots,\quad a''x+b''x'+c''x''+\dots,\dots$$

possono rappresentare un sistema qualunque di valori incongrui secondo il modulo m, dando ad x, x', x'' etc. dei convenienti valori incongrui secondo lo stesso modulo; perciò l'indicata espressione può rappresentare una sostituzione.

Questa condizione è necessaria; poichè se Δ ed m ammettessero un massimo comun divisore, per un dato sistema di valori di x, x', x'' etc. o non vi sarebbero valori di x, x', x'' etc. che sodisferebbero le (1), il che succederebbe se i secondi membri delle (1) non fossero divisibili per questo massimo comun divisore, ovvero vi sarebbero più sistemi di valori per x, x', x'' etc. che sodisferebbero le (1), ed in ambedue i casi l'indicata espressione non potrebbe rappresentare una sostituzione.

Corollario. — *Le sostituzioni della forma.*

$$B_{x \cdot x'} = (x, x', x'' \dots \quad x+x', x', x'')$$

$$B_{x' \cdot x} = (x, x', x'' \dots \quad x, x'+x, x'')$$

e le analoghe rappresentano delle sostituzioni, perchè il loro determinante è eguale ad 1.

115. Le sostituzioni di cui si è tenuto parola nel teorema precedente formano un gruppo di grado m^n, poichè il prodotto di due sostituzioni di questa forma conserva la forma medesima. A questo gruppo si è dato il nome di *gruppo lineare di grado* m^n.

116. Teorema 2°. — *Ogni sostituzione del gruppo lineare di grado* m^n *è uguale al prodotto di sostituzioni analoghe a* $B_{x \cdot x'}$, $B_{x' \cdot x}$ *etc. e di una sostituzione che lascia invariati tutti gl'indici ad eccezione dell'ultimo che moltiplica per un fattore costante.*

Supponiamo che gl'indici siano 3, e che si tratti della sostituzione

$$S = [x, x', x'' \quad ax+bx'+cx'',\quad a'x+b'x'+c'x'',\quad a''x+b''x'+c''x''] \pmod m.$$

Non vi può essere alcun divisore comune ad, a, b, c, m, poichè altrimenti non si potrebbero determinare per x, x', x'' dei valori che soddisfacessero la congruenza

$$ax+bx'+cx'' \equiv x_1 \pmod m$$

quando x_1 fosse primo con m.

Posta questa condizione si può sempre avere una sostituzione derivata da $B_{x \cdot x}$ e dalle analoghe che scambia l'indice x con l'altro $ax+bx'+cx''$. Infatti si ha

$$B^{l}_{x \cdot x'} = \left[x, x', x'' \quad x+lx', x', x''\right]$$

$$B^{1}_{x \cdot x'} B^{\delta}_{x' \cdot x} = \left[x, x', x'' \quad x+lx',\ \delta x + (1+l\delta)x', x''\right]$$

$$B^{l}_{x \cdot x'} B^{\delta}_{x' \cdot x} B^{\delta'}_{x'' \cdot x} = \left[x, x', a'' \quad x+lx',\ \delta x+(1+l\delta)x',\ \delta' x + l\delta' x' + x''\right]$$

$$\mathrm{B}_{x\cdot x'}^{l}\,\mathrm{B}_{x'\cdot x}^{\delta}\,\mathrm{B}_{x''\cdot x}^{\delta'}\,\mathrm{B}_{x\cdot x'}^{k}=\Big[x, x', x''\quad (1+k\delta)\,x+(k+l+lk\delta)\,x',$$
$$\delta x+(1+l\delta)\,x',\ \delta' x+l\delta' x'+x''\Big]$$

$$\mathrm{B}_{x\cdot x'}^{l}\,\mathrm{B}_{x'\cdot x}^{\delta}\,\mathrm{B}_{x''\cdot x}^{\delta'}\,\mathrm{B}_{x\cdot x'}^{k}\,\mathrm{B}_{x\cdot x''}^{k'}=\Big[x, x', x''\quad (1+k\delta+k'\delta')\,x+(l+k+kl\delta+k'l\delta')\,x'+k'x'',$$
$$\delta x+(1+l\delta)\,x',\ \delta' x+l\delta' x'+x''\Big]:$$

ora l'ultima di queste derivate, che indicheremo con T, scambierà x con $ax+bx'+cx''$ se potremo determinare $l, k, k', \delta, \delta'$ in modo che restino sodisfatte le congruenze

$$1+k\delta+k'\delta'\equiv a,\quad k+l\,(1+k\delta+k'\delta')\equiv b,\quad k'\equiv c \pmod m$$

ovvero l'equivalenti

$$1+k\delta+k'\delta'\equiv a,\quad k\equiv b-la,\quad k'\equiv c \pmod m.$$

Indichiamo con d il massimo comun divisore di c e di m, e con d_1 il risultato che si ottiene sopprimendo in d i fattori primi che dividono a e b. Se poniamo $l=d_1$ sarà k primo con d; infatti se q è un divisore di d che divide d_1, esso non può dividere b, quindi $b-d_1a$ non sarà divisibile per q; che se q non divide d_1, esso non può dividere simultaneamente a e b, perchè altrimenti a,b,c,m ammetterebbero un divisore comune, il che è impossibile, quindi un solo dei termini della differenza $b-d_1a$ sarà divisibile per q, per conseguenza questa differenza, ossia k_1, non sarà divisibile per q. Or poichè m, k, c non hanno alcun fattore comune, possiamo determinare tre numeri u, u', u'' tali che si abbia

$$mu+ku'+cu''=1,$$

e quindi si sodisferà alla congruenza

$$1+k\delta+k'\delta'\equiv a \pmod m$$

ponendo $\quad \delta\equiv(a-1)\,u',\quad \delta'\equiv(a-1)\,u'' \pmod m.$

Ciò posto la sostituzione $S_1=ST^{-1}$ rimpiazza prima gl'indici x, x', x'' rispettivamente cogl'altri

$$ax+bx'+cx'',\quad a'x+b'x'+c'x'',\quad a''x+b''x'+c''x'',$$

ed indi questi rispettivamente con x e con due funzioni lineari di x, x', x'', quindi non altera x o sarà della forma

$$S_1=[x, x', x''\quad x,\quad a_1'x+b_1'x'+c_1'x_1''\quad a_1''x+b_1''x'+c_1''x''].$$

Questa sostituzione risulta evidentemente da

$$S_2=[x, x', x''\quad x,\ b_1'x'+c_1'x'',\quad b_1''x'+c_1''x'']$$

e dall'altro due $\mathrm{B}_{x'\cdot x}^{a_1'}$, $\mathrm{B}_{x''\cdot x}^{a_1''}$, laonde sarà

$$S=S_2\,\mathrm{B}_{x'\cdot x}^{a_1'}\,\mathrm{B}_{x''\cdot x}^{a_1''}\,T.$$

Ora se nella sostituzione

$$T_1 = B^{m}_{x',x''} \; B^{n}_{x'',x'} \; B^{p}_{x',x''} = \left[x, x', x'' \quad x, (1+np)x' + (m+p+mnp)\,x'', nx' + (1+mn)x''\right]$$

determiniamo m, n, p colla condizione che restino sodisfatte le congruenze

$$1 + np \equiv b_1', \;\; m + p(1 + mn) \equiv c_1' \pmod m$$

ovvero
$$1 + np \equiv b_1', \;\; m \equiv c_1' - pb_1' \pmod m \;,$$

essa prenderà la seguente forma

$$T_1 = [x, x', x'' \quad x, b_1'x' + c_1'x'', \quad b_2''x' + c_2''x''],$$

ed allora la sostituzione $S_3 = S_2\,T_1^{-1}$ non altererà x ed x', e sarà della forma

$$S_3 = [x, x', x'' \quad x, x', b_3''x' + c_3''x''] \,;$$

ma quest'ultima sostituzione evidentemente risulta dalle due seguenti

$$\left[x, x', x'' \quad x, x', c''_3 x''\right], B^{b_3''}_{x'',x'} \,,$$

dunque il teorema è dimostrato.

117. Supponendo che il determinante delle quantità $\alpha, \beta \ldots\,; \alpha', \beta' \ldots\,; \ldots$ sia primo con m, le n congruenze

(1) $\quad y \equiv \alpha x + \beta x' + \ldots, \quad y' \equiv \alpha' x + \beta' x' + \ldots, \quad y'' \equiv \alpha'' x + \beta'' x' + \ldots, \ldots \pmod m$

sono soddisfatte da un sistema di valori di $x, x', \ldots$ qualunque siano i valori di y, y', y'' etc., e di qui risulta che se una quantita è distinta cogli indici x_1, x_1', x_1'' etc., indicando con x_2, x_2', x_2'' etc. i valori di x, x', x'' etc. che nelle (1) corrispondono ai valori x_1, x_1', x_1'' etc. di y, y', y'' etc., la medesima quantità potrà essere distinta cogli indici

$$\alpha x_2 + \beta x_2' + \ldots \;, \quad \alpha' x_2 + \beta' x_2' + \ldots, \quad \alpha'' x_2 + \beta'' x_2' + \ldots, \ldots$$

Ora la sostituzione

$$A = [x, x', \ldots \quad ax + bx' + \ldots, \quad a'x' + b'x' + \ldots, \ldots] \pmod m$$

cambia y in
$$\alpha(ax + bx' + \ldots) + \beta(a'x + b'x' + \ldots) + \ldots;$$

e sostituendo in questa espressione i valori di x, x' etc. tratti dalle (1), essa prenderà la forma $a_1 y + b_1 y' + \ldots$; analogamente A cambierà y', y'' etc. in altrettante funzioni di y, y' etc., quindi A si potrà porre sotto la seguente forma

$$A = [y, y', \ldots \; a_1 y + b_1 y' + \ldots, \quad a_1' y + b_1' y' + \ldots, \ldots] \pmod m$$

che dicesi trasformata della 1ª forma.

Da ciò che abbiamo detto risulta che quante volte tra due sistemi d'indici esistono delle relazioni condizionate come le (1), una sostituzione riferita ad uno di questi sistemi può essere trasformata in un'altra che sia riferita all'altro sistema.

118. Dicesi *caratteristica* della sostituzione A il determinante

$$\Delta = \begin{vmatrix} a - \mathrm{K} & a' & \dots \\ b & b' - \mathrm{K} & \dots \\ \dots & \dots & \dots \end{vmatrix}$$

in cui k è una quantità indeterminata.

Teorema 3.° — *La caratteristica di una sostituzione è uguale a quella di una qualunque delle sue trasformate.*

Poichè ogni sostituzione lineare è uguale (116) al prodotto di sostituzioni della forma $\mathrm{B}_{x' \cdot x}\ \mathrm{B}_{x \cdot x'}$ etc. e di un'altra che lascia inalterati tutti gl'indici ad eccezione dell'ultimo che moltiplica per una costante, si otterrà una trasformata qualunque della sostituzione A mediante delle successive trasformazioni nelle quali i nuovi indici sono collegati agli antichi con le relazioni seguenti,

$$y = x + x', \quad y' = x', \dots; \quad y = x, \quad y' = x + x', \dots; \dots$$
$$y = x, \quad y' = x', \dots y^{n-1} = rx^{n-1};$$

quindi sarà dimostrato il teorema enunciato, allorchè avremo dimostrato che la caratteristica di A è uguale a quella della sua trasformata quando tra i nuovi e gli antichi indici esistono le relazioni

$$y = \alpha x, \quad y' = x', \dots$$

ovvero l'altre
$$y = x + \beta x', \quad y' = x', \dots$$

Ora se esistono le prime relazioni la trasformata di A sarà

$$\left[y, y' \dots \quad \alpha\left(\frac{ay}{\alpha} + by' \dots\right), \ \left(\frac{a'y}{\alpha} + b'y' \dots\right), \dots\right]$$

e la corrispondente caratteristica sarà

$$\begin{vmatrix} a - \mathrm{K} & \dfrac{a'}{\alpha} & \dots \\ \alpha b & b' - \mathrm{K} & \dots \\ \dots & \dots & \dots \end{vmatrix} = \frac{1}{\alpha} \begin{vmatrix} \alpha(a - \mathrm{K}) & a' & \dots \\ \alpha b & b' - \mathrm{K} & \dots \\ \dots & \dots & \dots \end{vmatrix} = \begin{vmatrix} a - \mathrm{K} & a' & \dots \\ b & b' - \mathrm{K} & \dots \\ \dots & \dots & \dots \end{vmatrix}.$$

E se esistono le seconde relazioni la trasformata di A cambierà $y, y' \dots$ in

$$(a + \beta a')\, x + (b + \beta b')\, x' + \dots \equiv (a + \beta a')\, y + [b + \beta b' - \beta(a + \beta a')]\, y' + \dots$$
$$a'x + b'x' + \dots \equiv a'y + (b' - \beta a')\, y' + \dots$$

e la caratteristica corrispondente sarà il determinante

$$\begin{vmatrix} a + \beta a' - \mathrm{K} & a' & \dots \\ b + \beta b' - \beta(a + \beta a') & b' - \beta a' - \mathrm{K} & \dots \\ \dots & \dots & \dots \end{vmatrix}.$$

Aggiungendo a ciascun elemento della seconda linea orizzontale l'elemento corrispondente della prima moltiplicato per la costante β, esso si trasforma nell'altro

$$\begin{vmatrix} a+\beta a'-K & a' & \dots \\ b+\beta b'-\beta K & b'-K & \dots \\ \dots & \dots & \dots \end{vmatrix}$$

il quale si trasforma nell'altro

$$\begin{vmatrix} a-k & a' & \dots \\ b & b'-K & \dots \\ \dots & \dots & \dots \end{vmatrix}$$

se togliamo da ciascun elemento della prima colonna verticale l'elemento corrispondente della seconda colonna moltiplicato per β.

CAPO 3.°

Ordine del gruppo lineare.

119. Teorema. — *L'ordine* $\Omega(m^n)$ *del gruppo lineare di grado* m^n *è uguale ad*

$$(m, n)\, m^{n-1}\, (m, n-1)\, m^{n-2} \dots (m, 1),$$

dinotandosi con (m, p) *il numero dei sistemi di* p *numeri inferiori ad* m *e che hanno un massimo comun divisore primo con* m.

Siano 1, R_1, R_2 ... le sostituzioni del gruppo in parola che non variano la x, N il loro numero e T una sostituzione che cambia x in $ax+bx'+cx''+\dots$ Le sostituzioni del gruppo che scambiano x in $ax+bx'+cx''+\dots$ sono soltanto le seguenti

$$T, \quad TR_1, \quad TR_2, \dots$$

Infatti sia

$$U=[x,x',x''\dots \quad ax+bx'+cx''+\dots, \quad a_1'x+b_1'x'+c_1'x''+\dots, \quad a_1''x+b_1''x'+c_1''x''+\dots,\dots]$$

una sostituzione del gruppo lineare, e supponiamo che T^{-1} scambi x, x', x'' ... rispettivamente in

$$\varphi(x, x', x'', \dots), \quad \varphi_1(x, x', x'', \dots), \quad \varphi_2(x, x', x'', \dots), \dots,$$

allora $T^{-1}U$ scambierà x in

$$a\varphi(x, x', x'', \dots)+b\varphi_1(x, x', x'', \dots)+c\varphi_2(x, x', x'', \dots)+\dots \equiv x, \pmod{m}$$

e perciò apparterrà alla serie 1, R_1, R_2 etc., ed U farà parte dell'altra T, TR_1, TR_2 etc.

Ma nell'espressione $ax+bx'+cx''+\dots$ possiamo dare ad a, b, c, ... tutti gli (m, n) sistemi di valori minori di m e che hanno un massimo comun divisore primo con m, dunque per ciascuno di questi sistemi si avranno $N(m, n)$ sostituzioni diverse.

Ora le sostituzioni che non alterano l'indice x sono della forma

$$[x, x', x'' \dots \quad x, a'x+b'x'+c'x''+\dots, \quad a''x+b''x'+c''x''+\dots, \dots],$$

quindi vi sono tante sostituzioni che non alterano x quanti sono i sistemi di va-

lori di $a', b', c', \ldots$; $a'', b'', c'', \ldots$; ... i quali sono minori di m e danno pel determinante

$$\begin{vmatrix} 1 & 0 & 0 & \ldots\ldots \\ a' & b' & c' & \ldots\ldots \\ a'' & b'' & c'' & \ldots\ldots \\ \ldots & \ldots & \ldots & \ldots \end{vmatrix}$$

un valore che è primo con m, ma questo determinante è uguale all'altro

$$\Delta = \begin{vmatrix} b' & c' & \ldots\ldots \\ b'' & c'' & \ldots\ldots \\ \ldots & \ldots & \ldots \end{vmatrix},$$

dunque il numero delle sostituzioni che non alterano x è uguale al numero dei sistemi di valori di a', a'', etc. minori di m, cioè m^{n-1}, moltiplicato pel numero dei sistemi di valori di $b', c', \ldots$; $b'', c'', \ldots$; ... che danno pel precedente determinante un valore che è primo con m, ma, corrispondendo Δ al gruppo lineare di grado m^{n-1}, vi sono per $a', b', \ldots$; $a'', b'', \ldots$; ... $\Omega(m^{n-1})$ sistemi di valori, adunque sarà

$$N = m^{n-1}\,\Omega(m^{n-1}),$$

e quindi $$\Omega(m^n) = (m, n)\, m^{n-1}\,\Omega(m^{n-1}).$$

Similmente sarà

$$\Omega(m^{n-1}) = (m, n-1)\, m^{n-2}\,\Omega(m^{n-2})$$

e così di seguito, per modo che sarà

$$\Omega(m^n) = (m, n)\, m^{n-1}\,(m, n-1)\, m^{n-2} \ldots \Omega(m);$$

ma $\Omega(m)$ rappresenta l'ordine del gruppo lineare le cui sostituzioni sono della forma

$$[x, ax] \pmod m,$$

quindi deve essere uguale al numero dei valori di a che sono minori di m e primi con m, ma questo numero è indicato dal simbolo $(m, 1)$, dunque sarà

$$\Omega(m^n) = (m, n)\, m^{n-1}\,(m, n-1)\, m^{n-2} \ldots (m, 1).$$

120. Osservazione. — È facile il calcolare il valore di (m, μ), essendo $m = p^{\lambda} p'^{\lambda'} p''^{\lambda''} \ldots$

Per ottenere (m, μ) bisogna togliere dal numero m^{μ} dei sistemi di μ numeri minori di m quello dei sistemi di μ numeri che ammettono un massimo comun divisore il quale abbia per fattori uno o più dei numeri p, p', p'' etc. Ora $\frac{m}{p}, \frac{m}{pp'}, \frac{m}{pp'p''}$ etc. dinotano quanti numeri minori di m sono divisibili rispettivamente per $p, pp', pp'p''$ etc., e quindi $\left(\frac{m}{p}\right)^{\mu}, \left(\frac{m}{pp'}\right)^{\mu}, \left(\frac{m}{pp'p'}\right)^{m}$ etc. dinotano quanti sono i sistemi di μ numeri minori di m che hanno un massimo comun divisore che sia divisibile rispettivamente per $p, pp', pp'p''$ etc. Inoltre un numero divisibile pel prodotto di n fattori di m può essere considerato come divisibile pel prodotto di $p < n$ fattori di m in

tanti modi diversi quante sono le combinazioni a p a p di n lettere. Ma i coefficienti dei termini dello sviluppo di $(a-b)^n$, a partire dal secondo, dinotano i numeri delle combinazioni ad uno ad uno, a due a due etc. ad n ad n di n lettere, e la loro somma è uguale a -1; dunque sarà

$$(m, \mu) = m^\mu - \left(\frac{m}{p}\right)^\mu - \left(\frac{m}{p'}\right)^\mu - \ldots + \left(\frac{m}{pp'}\right)^\mu + \ldots - \left(\frac{m}{pp'p''}\right)^\mu - \ldots$$

$$= m^\mu \left(1 - \frac{1}{p^\mu}\right)\left(1 - \frac{1}{p'^\mu}\right)\ldots$$

Se $m = pq$, sarà $\qquad (m, \mu) = (p, \mu)(q, \mu)$,

e quindi $\qquad \Omega(m^n) = \Omega(p^n)\,\Omega(q^n)$.

Se m è uguale al numero primo p, sarà

$$(p, \mu) = p^\mu - 1,$$

ed $\quad \Omega(p^n) = (p^n - 1)\,p^{n-1}(p^{n-1} - 1)\,p^{n-2} \ldots = (p^n - 1)(p^n - p) \ldots (p^n - p^{n-1})$.

Questo risultato è stato scoverto da Galois ed è stato dimostrato da Betti.

CAPO 4.°

Fattori di composizione del gruppo lineare.

121. Nella ricerca dei fattori di composizione del gruppo lineare G di grado m^n si possono distinguere tre casi: 1° che m sia un numero primo: 2° che m sia una potenza di un numero primo: 3° che m sia un numero composto.

1° Caso $m = p$, essendo p un numero primo.

Teorema. — *Siano α, β, γ etc. i fattori primi di* $p-1$, *ed* α', β', γ' *etc. quelli del massimo comun divisore δ tra* $p-1$ *ed* n; *saranno*

$$\alpha, \beta, \gamma, \ldots \frac{\Omega(p^n)}{(p-1)\delta}, \alpha', \beta', \gamma', \ldots$$

i fattori di composizione del gruppo lineare di ordine p^n, *eccetto i casi di* $p^n = 2^2$ *e di* $p^n = 3^2$.

Indichiamo con r una radice primitiva della congruenza

$$x^{p-1} \equiv 1 \pmod{p}$$

Le prime $p-1$ potenze di r sono congrue secondo il modulo p ai numeri $1, 2, \ldots p-1$, quindi un numero qualunque primo con p è congruo secondo il modulo p ad una di queste potenze. Ora una sostituzione che lascia inalterati tutti gl'indici eccetto l'ultimo che moltiplica per una quantità c è identica ad un'altra della stessa forma in cui il moltiplicatore dell'ultimo indice è congruo secondo il modulo p a c. Ma una sostituzione lineare si può mettere sempre sotto la forma $S = \Sigma\theta$ in cui Σ è una sostituzione che lascia invariati tutti gl'indici eccetto l'ultimo che moltiplica per una data quantità, e θ è una derivata da $B_{x,x'}$ e dalle ana-

logho, inoltre il determinante di S è il moltiplicatore dell'ultimo indice in Σ. Quindi tutte le sostituzioni lineari i cui determinanti sono congrui ad una medesima potenza di r risultano dal moltiplicare la sostituzione della forma Σ in cui il moltiplicatore dell'ultimo indice è questa potenza di r per tutte le derivate da $B_{x',x'}$ e dalle analoghe, laonde ad ogni potenza di r corrisponde un medesimo numero di sostituzioni lineari, ma le potenze di r^{α}, $r^{\alpha\beta}$, $r^{\alpha\beta\gamma}$ etc. formano rispettivamente la α^{ma}, $\alpha\beta^{ma}$, $\alpha\beta\gamma^{ma}$ etc. parte delle $p-1$ potenze di r; dunque gl'ordini dei gruppi G_{α}, $G_{\alpha\beta}$, $G_{\alpha\beta\gamma}$, ... Γ formati da tutte le sostituzioni di G che hanno rispettivamente per determinante una potenza di $r^{\alpha}, r^{\alpha\beta}, r^{\alpha\beta\gamma}, \ldots, r^{p-1}$ saranno rispettivamente

$$\frac{\Omega(p^n)}{\alpha}, \ \frac{\Omega(p^n)}{\alpha\beta}, \ \frac{\Omega(p^n)}{\alpha\beta\gamma}, \ldots\ldots, \frac{\Omega(p^n)}{p-1}.$$

Or se indichiamo con r' una radice primitiva della congruenza

$$x^{\delta} \equiv 1 \pmod p,$$

le potenze di $r'^{\alpha'}$, $r'^{\alpha'\beta'}$, $r'^{\alpha'\beta'\gamma'}$ etc. saranno rispettivamente la α'^{ma}, $\alpha'\beta'^{ma}$, $\alpha'\beta'\gamma'^{ma}$ etc. parte di δ, quindi gl'ordini dei gruppi H_{δ}, $H_{\alpha'}$, $H_{\alpha'\beta'}$, $H_{\alpha'\beta'\gamma'}$ etc. le cui sostituzioni moltiplicano tutti gl'indici rispettivamente per una medesima potenza di r', $r'^{\alpha'}$, $r'^{\alpha'\beta'}$, $r'^{\alpha'\beta'\gamma'}$ etc. saranno rispettivamente

$$\delta, \frac{\delta}{\alpha'}, \ \frac{\delta}{\alpha'\beta'}, \ \frac{\delta}{\alpha'\beta'\gamma'}, \text{ etc.}$$

122. Da quanto si è detto risulta che si potrà conchiudere essere

$$\alpha, \beta, \gamma \ldots \frac{\Omega(p^n)}{(p-1)\delta}, \alpha', \beta', \gamma' \ldots$$

i fattori di composizione di G, quando si sarà dimostrata la seguente proposizione.

I gruppi

$$G, G_{\alpha}, G_{\alpha\beta} \ldots \Gamma, H_{\delta}, H_{\alpha'}, H_{\alpha'\beta'}, \ldots \tag{1}$$

sono così condizionati: 1° che ciascuno sia contenuto nel precedente e sia permutabile alle sue sostituzioni: 2° che sia il più generale di quelli che godono di questa doppia proprietà.

Consideriamo due gruppi successivi G_{α} e $G_{\alpha\beta}$ della parte della (1) che comincia con G e termina a Γ. Sia S una sostituzione del primo ed S' una sostituzione del secondo, $r^{m\alpha}$ il determinante dell'una ed $r^{m'\alpha\beta}$ quello dell'altra. Poichè $r^{m'\alpha\beta}$ è una potenza di r^{α}, S' è contenuta in G_{α} e quindi $G_{\alpha\beta}$ in G_{α}. Inoltre essendo $\frac{1}{r^{m\alpha}}$ il determinante di S^{-1} quello di $S^{-1}S'S$ sarà $r^{m'\alpha\beta}$, perciò $S^{-1}S'S$ appartiene a $G_{\alpha\beta}$ e per conseguenza $G_{\alpha\beta}$ è permutabile ad ogni sostituzione di G_{α}. Infine non vi può essere un gruppo intermedio a G_{α} ed a $G_{\alpha\beta}$, poichè se vi fosse il suo ordine dovrebbe essere un numero che contenesse $\frac{\Omega(p^n)}{\alpha\beta}$ e fosse contenuto in $\frac{\Omega(p^n)}{\alpha}$, il che è impossibile per essere β un numero primo.

In un modo non meno facile del già seguito si dimostrerebbe che sono nelle stesse condizioni di G_{α} e di $G_{\alpha\beta}$ due gruppi consecutivi scelti nella parte della (1)

che comincia da H_δ e va sino alla fine; come pure che H_δ è contenuto in Γ ed è permutabile ad ognuna delle sue sostituzioni; quindi resta a dimostrare che tra Γ ed H_δ non vi può essere un gruppo che gode della doppia proprietà in parola.

123. Supponiamo $n = 3$. Sia

$$S=[x, x', x'', \quad ax+bx'+cx'', \quad a'x+b'x'+c'x'', \quad a''x+b''x'+c''x'']$$

una sostituzione appartenente ad un gruppo I intermedio a Γ ed ad H_δ, la quale non moltiplichi tutti gl'indici per un medesimo fattore.

Poichè le sole sostituzioni di H_δ sono mutabili con l'altre $B_{x.x'}$, $B_{x'.x}$ etc., non lo sarà S che non fa parte di H_δ, quindi

$$T = S^{-1}B^{-1}_{x.x'}SB_{x.x'}$$

non sarà uguale ad 1 ed apparterrà ad I, perchè, essendo $B_{x.x'}$ una sostituzione di Γ, la trasformata $B^{-1}_{x.x'}SB_{x.x'}$ per ipotesi è contenuta in I come anche S^{-1}. Ora se supponiamo che X_1, X_2, X_3 siano le funzioni lineari di x, x', x'' che S^{-1} fa succedere ad x, x', x'' sarà

$$S^{-1} = [x, x', x'' \quad X_1, X_2, X_3]$$

$$S^{-1}B^{-1}_{x.x'} = [x, x', x'' \quad X_1 - X_2, \; X_2, X_3]$$

$$S^{-1}B^{-1}_{x.x'}S = [x, x', x'' \quad a(X_1 - X_2) + bX_2 + cX_3, \quad a'(X_1 - X_2) + b'X_2 + c'X_3,$$
$$a''(X_1 - X_2) + b''X_2 + c''X_3],$$

ma $aX_1 + bX_2 + cX_3 \equiv x, \quad a'X_1 + b'X_2 + c'X_3 \equiv x', \quad a''X_1 + b''X_2 + c''X_3 \equiv x'' \pmod p$,

quindi sarà $S^{-1}B^{-1}_{x.x'}S = [x, x', x'' \quad x - aX_2, \; x' - a'X_2, \quad x'' - a''X_2]$,

e per conseguenza, ponendo

$$x - aX_2 + x' - a'X_2 = \alpha x + \beta x' + \gamma x'',$$

sarà $T = S^{-1}B^{-1}_{x.x'}SB_{x'.x} = [x, x', x'' \quad \alpha x + \beta x' + \gamma x'', \quad x' - a'X_2, \; x'' - a''X_2]$.

Se $a' \equiv a'' \equiv 0$, dovrà essere $\alpha \equiv 1$, perchè il determinante di T deve essere congruo ad 1 per essere T una sostituzione di Γ. Inoltre possiamo supporre $\beta \equiv 1$, $\gamma \equiv 0$; poichè se fosse $\gamma \gtrless 0 \pmod p$ potremo prendere x, $\beta x' + \gamma x''$, x'' per indici in luogo di x, x', x'', ed allora T prenderebbe la forma seguente

$$T = [x, x', x'' \quad x + x', \; x', x''].$$

Ma Γ contiene la sostituzione

$$[x, x', x'' \quad x', \; x_1 - x'']$$

e l'analoghe, quindi I dovrà contenere la trasformata di T per mezzo di queste sostituzioni, le trasformate di queste trasformate etc., ma tra queste si trovano $B_{x'.x}B_{x'.x}$ etc., dunque I conterrà tutte quest'ultime sostituzioni; ma, potendo ogni sostituzione lineare mettersi sotto la forma $\Sigma\theta$ in cui Σ è una sostituzione della forma

$$[x, x', x'' \quad x, x', cx'']$$

e θ una derivata da $B_{x.x'}$ e dall'analoghe, tutte le sostituzioni di Γ sono della forma θ, perchè i loro determinanti c sono uguali ad 1, adunque I si confonde con Γ.

Se si suppone che a' fosse diversa da zero, prendendo per indici indipendenti

$$x,\ x',\ x'' - \frac{a''}{a'}x' = u,$$

sarà $$T = [x, x', u \quad a_1 x + b_1 x' + c_1 u,\ \ a_1' x + b_1' x' + c_1' u,\ \ u]$$

e quindi $$T_1 = T^{-1}B^{-1}_{x \cdot u} T B_{x \cdot u} = [x, x', u \quad x - (a_1 - 1)u,\ \ x' - a_1' u,\ \ u].$$

Ora è evidente che non possa essere

$$a_1 - 1 \equiv 0, \quad a'_1 \equiv 0$$

perchè T_1 è diversa da 1. Supponiamo che a_1' sia diversa da zero. Trasformiamo T_1 scambiando gl'indici x, x', u negli altri

$$y = x - \frac{a_1 - 1}{a_1'}x', \qquad y' = \frac{-x'}{a_1'}$$

ed abbiamo la trasformata

$$T_1 = [y, y', u \quad y,\ y' + u,\ u]$$

la quale combinata colle sue trasformate per mezzo delle sostituzioni di Γ riproduce tutte queste ultime.

124. Non essendo la dimostrazione testè fatta applicabile quando il numero degl'indici fosse uguale a 2, passiamo a trattare questo caso.

Sia S una sostituzione di Γ che non moltiplichi tutti gl'indici per una stessa quantità. Evidentemente vi sarà una funzione y degl'indici x ed x' la quale non darà un risultato della forma ry quando su di essa si opererà la sostituzione S, quindi se indichiamo con y' questo risultato si potrà porre S sotto la forma

$$S = [y, y' \quad y', \quad cy + dy'].$$

Dovendo essere uguale ad 1 il determinante di questa sostituzione sarà $c = 1$. La quantità d può essere diversa da zero, ovvero uguale a zero.

1.° Sia d diversa da zero, Γ contiene la sostituzione

$$T = [y, y' \quad \alpha y, \quad \alpha^{-1} y]$$

perciò Γ contiene l'altra

$$U = T^{-1}STS = [y, y' \quad -\alpha^2 y, \quad -\alpha(1 + \alpha^{-2})y - \alpha^2 y']$$

e quindi U^2. Or se poniamo $\alpha \equiv 1$ e sostituiamo all'indice y l'altro $z \equiv hdy$, il che è permesso quando $p > 2$ e non quando $p = 2$ perchè tutt'i valori di y corrisponderebbero al valore 0 di z, allora U^2 prenderà la forma

$$U^2 = [z, y' \quad z.\ y' + z],$$

e combinando questa sostituzione colle sue trasformate per mezzo delle sostituzioni di Γ si riprodurrà questo gruppo.

2.° Sia $d \equiv 0$. Se $p > 5$ possiamo scegliere α in modo che sia $\alpha^4 \gtrless 1$, e se indichiamo con β un numero intero tale che si abbia

$$\beta(\alpha^4 - 1) \equiv 0 \pmod{p}$$

I conterrà la sostituzione

$$(B^{-1}_{y,y'} U B_{y,y'} U^{-1})^3 = B_{y,y'}$$

la quale combinata colle sue trasformate per mezzo delle sostituzioni di Γ riprodurrà questo gruppo.

3.° Sia $d \equiv 0$, $p = 5$. Se si prendono per indici indipendenti

$$z \equiv 2y + y', \quad z' \equiv -2y + y'$$

la S cambierà z e z' rispettivamente in

$$2y' + y, \quad -2y' - y,$$

e sostituendo in quest'espressioni i valori di y e di y' tratti dalle precedenti congruenze

$$y \equiv \frac{z - z'}{4}, \quad y' \equiv \frac{z + z'}{4},$$

si avrà

$$\frac{3z + 5z'}{4}, \quad \frac{-5z - 3z'}{4},$$

ma poichè si suppone il modulo p uguale a 5, si può sopprimere $5z'$ nella 1ª di queste ultime espressioni e $-5z$ nella 2ª, e possiamo sostituire $3 + 5$ a 3, allora le dette espressioni si riducono a $2z$ ed a $-2z'$ ed S prenderà la forma

$$S = [z, z' \quad 2z, \quad -2z'].$$

Ora I contiene la sostituzione

$$T_2 = B_{z,z'} S^{-1} B^{-1}_{z,z'} S = [z, z' \quad z + 2z', \ z']$$

e quindi l'altra

$$T_2^3 = [z, z' \quad z + 6z', \ z'] = [z, z' \quad z + z', \ z'] \pmod{p},$$

laonde I contiene tutte le trasformate di T_2^3 per mezzo delle sostituzioni di Γ, perciò si confonde con Γ.

125. Se $p^n = p^2$ il gruppo G sarà di ordine $(2^2 - 1)(2^2 - 2) = 6$, e si verifica che le sue sostituzioni sono permutabili al gruppo formato dalle potenze della sostituzione $[x, x' \ x', \ x + x']$, ma l'ordine di questo ultimo gruppo è 3, dunque i fattori di composizione di G saranno 2 e 3.

Se $p^n = 3^2$ si verifica: 1° che le sostituzioni di G in numero $(3^2-1)(3^2-3)=48$ derivano dalle seguenti

$$A = \begin{vmatrix} x & 2x \\ x' & x+x' \end{vmatrix}, \quad B = \begin{vmatrix} x & x' \\ x' & 2x+x' \end{vmatrix}, \quad C = \begin{vmatrix} x & -x' \\ x' & x \end{vmatrix}, \quad D = \begin{vmatrix} x & x+x' \\ x' & x-x' \end{vmatrix}, \quad E = \begin{vmatrix} x & 2x \\ x' & 2x' \end{vmatrix}:$$

2° che i gruppi

$$G = (A, B, C, D, E), \quad (B, C, D, E), \quad (C, D, E), \quad (D, E), \quad (E)$$

hanno rispettivamente per ordine 48, 24, 8, 4, 2: 3° che ciascuno è permutabile alle sostituzioni del precedente. Quindi i fattori di composizione di G saranno 2, 3, 2, 2,

126. 2° Caso $m = p^\lambda$. Ad ogni sostituzione

$$[x, x', \dots \quad ax + bx' + \dots, \quad a'x + b'x' + \dots, \dots] \pmod{p^\lambda}$$

del gruppo lineare G di grado $p^{\lambda n}$ corrisponde una sostituzione

$$[y, y', \ldots \quad ay + by' + \ldots, \quad a'y + b'y' + \ldots, \ldots] \pmod{p}$$

del gruppo lineare I di grado p^n. Inoltre è evidente che al prodotto di due sostituzioni di G corrisponda il prodotto delle due corrispondenti di I, quindi I è isoformo a G.

Scomponiamo il gruppo I negli altri

$$I, \quad I_\alpha, \quad I_\beta, \quad I_\gamma, \ldots\ldots 1 \qquad (2)$$

tali: 1° che ciascuno sia contenuto nel precedente e sia permutabile alle sue sostituzioni: 2° che sia il più generale di quelli che godono questa doppia proprietà. Indichiamo con

$$G_\alpha, \quad G_\beta, \quad G_\gamma, \ldots \ldots M$$

i gruppi delle sostituzioni di G che corrispondono a quelle di I che compongono rispettivamente i gruppi

$$I_\alpha, \quad I_\beta, \quad I_\gamma, \ldots\ldots 1.$$

Dico che i gruppi

$$G, \quad G_\alpha, \quad G_\beta, \quad G_\gamma, \ldots\ldots M$$

sono condizionati nello stesso modo di quelli che formano la serie (2).

Consideriamo i gruppi G_α e G_β. Indichiamo con S una sostituzione del 1°, con S' una del 2°, con S_1 ed S_1' le corrispondenti appartenenti rispettivamente ad I_α ed I_β. Poichè la sostituzione S^{-1} di G_α corrisponde all'altra S_1^{-1} di I_α, ad $S^{-1}S'S$ corrisponderà $S_1^{-1}S_1'S_1$ che evidentemente appartiene ad I_β e perciò $S^{-1}S'S$ dovrà appartenere a G_β, quindi G_β è permutabile alle sostituzioni di G_α.

Inoltre tra G_α e G_β non vi può essere un gruppo intermedio che fosse permutabile alle sostituzioni di G_α, perchè altrimenti tra I_α ed I_β vi dovrebbe essere un gruppo permutabile alle sostituzioni di I_α, il che è impossibile.

Or se indichiamo con f, f', f'' etc. i fattori di composizione di I, saranno gli ordini di $I_\alpha, I_\beta, I_\gamma$ etc. rispettivamente la $f^a, ff'^a, ff'f''^a$ etc. parte dell'ordine di I_1 ma ad ogni sostituzione di I corrisponde un medesimo numero di sostituzioni di G, dunque gl'ordini di G_α, G_β, G_γ etc. saranno rispettivamente la $f^a, ff'^a, ff'f''^a$ etc. parte dell'ordine di G, ossia i fattori di composizione di G saranno quelli stessi di I e quelli di M.

127. ***I fattori di composizione di M sono tutti eguali a*** **p.**

Le sostituzioni di M, dovendo corrispondere alla sostituzione 1 di I sono della forma

$$T = [x, x' \ldots \quad x + p\,(ax + bx' + \ldots), \quad x' + p\,(a'x + b'x' + \ldots), \ldots] \pmod{p^\lambda}$$

quindi M contiene un gruppo M_1 le cui sostituzioni sono della forma

$$T_1 = [x, x' \ldots \quad x + p^2\,(a_1x + b_1x' + \ldots), \quad x' + p^2\,(a_1'x + b_1'x' + \ldots), \ldots] \pmod{p^\lambda},$$

M_1 contiene un gruppo M_2 le cui sostituzioni sono della forma

$$T_2 = [x, x' \ldots \quad x + p^3\,(a_2x + b_2x' + \ldots), \quad x' + p^3\,(a_2'x + b_2'x' + \ldots), \ldots] \pmod{p^\lambda},$$

e così di seguito sino ad un gruppo $M_{\lambda-3}$ che ne contiene un altro $M_{\lambda-2}$ le cui sostituzioni sono della forma

$$T_{\lambda-2}=[x, x' \dots \quad x+p^{\lambda-1}(a_{\lambda-2}x+b_{\lambda-2}x'+\dots), \quad x'+p^{\lambda-1}(a'_{\lambda-2}x+b'_{\lambda-2}x'+\dots), \dots] \pmod{p^\lambda}.$$

È facile il vedere: 1° che le sostituzioni di quest'ultima forma sono mutabili con quelle di M: 2° che tra due sostituzioni T', T'' di M ed un'altra T_1 di M_1 esista la relazione

$$T' T'' = T'' T' T_1 :$$

3° che tra tre sostituzioni $T^{(r)}$, T_r, T_{r+1} appartenenti rispettivamente ai tre gruppi M, M_r, M_{r+1} esista la relazione

$$T_r T^{(r)} = T^{(r)} T_r T_{r+1},$$

da cui si deduce che alle sostituzioni di M sono permutabili i gruppi M_1, M_2 etc.: infatti da essa si ricava

$$(T^{(r)})^{-1} T_r T^{(r)} = T_r T_{r+1},$$

ma $T_r T_{r+1}$ è una sostituzione di M_r, perchè M_r comprende M_{r+1}, dunque la precedente relazione dimostra che la trasformata di una sostituzione di M_r per mezzo di una sostituzione qualunque di M appartiene ad M_r, perciò M_r è permutabile alle sostituzioni di M.

Or supponiamo che A sia una sostituzione di M che non appartenga ad M_1. Vi dovranno essere delle potenze di A che apparterranno ad M_1 (*). Supponiamo che la minima sia A^r. Si può supporre che r sia un numero primo, poichè se fosse uguale ad mr, essendo m un numero primo, potremo prendere A^r in luogo di A, ed allora il grado della potenza di A^r che darebbe una sostituzione appartenente ad M_1 sarebbe il numero primo m.

Le sostituzioni della forma $A^\rho T_1$ in cui ρ è minore di r sono tutte distinte. Infatti se fosse

$$A^{\rho'} T_1 = A^{\rho''} T'_1$$

sarebbe anche

$$A^{\rho'-\rho''} = T_1' T_1^{-1},$$

ma $\rho' - \rho''$ è minore di r, quindi non sarebbe r il minimo esponente a cui bisognerebbe innalzare A per avere la sostituzione $T_1' T_1^{-1}$ di M_1, il che è contrario all'ipotesi fatta.

Inoltre il prodotto di due sostituzioni $A^{\rho_1} T_1$, $A^{\rho_2} T_1'$ della forma $A^\rho T_1$ ha la medesima forma. Infatti questo prodotto è $A^{\rho_1} T_1 A^{\rho_2} T_1'$, ma essendo M_1 permutabile alle sostituzioni di M si ha

$$T_1 A^{\rho_2} = A^{\rho_2} T_1'',$$

quindi questo prodotto si può mettere sotto la forma $A^{\rho_1+\rho_2} T_1'' T_1'$, ovvero sotto l'altra $A^{\rho_3} A^r A_1'' T_1'$, supponendo essere $\rho_1 + \rho_2 = r + \rho_3$, ma $A^r A_1'' T_1'$ è una sostituzione di M_1, dunque il prodotto in parola si può mettere sotto la forma $A^\rho T_1$,

(*) Infatti essendo il gruppo M_1 contenuto in M, pel teorema di Lagrange, la sostituzione A non contenuta in M_1 si può mettere sotto la forma CT_1 essendo C una sostituzione di M non contenuta in M_1: or poichè M_1 è permutabile alle sostituzioni di M, la potenza m^{ma} di CT_1 si può mettere sotto la forma $C^m T_1^{(n)}$, essendo $T_1^{(n)}$ una sostituzione di M_1, e se si suppone che m sia l'ordine di C sarà $C^m = 1$, ed $A^m = T_1^{(n)}$.

laondo le sostituzioni di questa forma costituiscono un gruppo N di ordine μr, indicando con μ l'ordine di M_1.

Supponiamo che B sia una sostituziono di M che non sia della forma $A^\rho T_1$ e che sia B^s la minima potenza di B che si riduce a questa forma (*). Per una ragiona analoga a quella innanzi indicata possiamo supporre che s sia un numero primo. Si dimostrerebbe come si è fatto innanzi che le sostituzioni della forma $B^\sigma A^\rho T_1$ in cui σ è minore di s formano un gruppo il di cui ordine è μrs.

Continuando allo stesso modo si giungerà ad una forma sotto la quale si possono porre tutte le sostituzioni di M. Supponiamo per fissare le idee che questa sia $B^\sigma A^\rho T_1$. Allora tra due dei tre gruppi M, N, M_1 non ve ne può essere un altro, perchè, se vi fosse, il suo ordine dovrebbe essere un divisore di μrs ed un multiplo di μr, il che è impossibile per essere s numero primo.

Inoltre alle sostituzioni di uno di questi tre gruppi, per esempio a quelle di M è permutabile il seguente N. Infatti la trasformata di $A^\rho T_1$ per mezzo di $B^{\sigma'} A^{\rho'} T_1'$ è

$$(B^{\sigma'} A^{\rho'} T_1')^{-1} A_\rho T_1 B^{\sigma'} A^{\rho'} T_1'$$

ovvero

$$(A^{\rho'} T_1')^{-1} (B^{\sigma'})^{-1} A_\rho T_1 B^{\sigma'} A^{\rho'} T_1',$$

essendo

$$(B^{\sigma'} A^{\rho'} T_1')^{-1} = (A^{\rho'} T_1')^{-1} (B^{\sigma'})^{-1},$$

ma

$$(B^{\sigma'})^{-1} A^\rho T_1 B^{\sigma'} = (B^{\sigma'})^{-1} A^\rho B^{\sigma'} (B^{\sigma'})^{-1} T_1 B^{\sigma'}$$

$$(B^{\sigma'})^{-1} A^\rho B^{\sigma'} = A^\rho T_1'', \quad (B^{\sigma'})^{-1} T_1 B^{\sigma'} = T_1'''$$

dunque la trasformata sarà uguale ad

$$(A^{\rho'} T_1')^{-1} A^\rho T_1'' T_1''' A^{\rho'} T_1'$$

e perciò apparterrà ad N.

Dal ragionamento fatto risulta che i tre gruppi M, N, M_1 sono così condizionati che ciascuno è contenuto nel precedente, è permutabile alle sue sostituzioni, ed è il più generale di quelli che godono questa doppia proprietà; dunque i fattori di composizione di M sono r, s o quelli di M_1.

Ora il determinante di una sostituzione della forma

$$[x, x', \ldots \quad x + p\,(ax + bx' + \ldots), \quad x' + p\,(a'x + b'x' + \ldots), \ldots]$$

è uguale ad una espressione della forma $1+pD$, essendo D una funzione di a, b, etc., quindi esso è primo con p, qualunque sia il valore di D, per conseguenza possiamo dare a ciascuno degli n^2 coefficienti a, b, etc. tutt'i valori da 0 a $p^{\lambda-1}-1$, perciò l'ordine di M sarà $p^{(\lambda-1)n^2}$, ma r ed s sono due numeri primi che dividono l'ordine di M, dunque $r = s = p$. Analogamente si dimostra che i fattori di composizione di M_1 sono gli uni uguali a p e gli altri a quelli di M_2 etc.

128. 3° Caso $m = \alpha^\lambda \beta^\mu \gamma^\rho \ldots$ Poniamo $p = \beta^\mu \gamma^\rho \ldots$, $q = \alpha^\lambda$ donde $m = pq$.

(*) Questa 2ª ipotesi può farsi, poichè essendo il gruppo N contenuto in M una sostituzione B di M può mettersi sotto la forma $DA^\rho T_1$; e poichè tra due sostituzioni T′, T″ di M ed un'altra T_1 di M_1 si ha la relazione $T'T'' = T''T'T_1$, ed è M_1 permutabile alle sostituzioni di M, la potenza m^{ma} di B si può mettere sotto la forma $D^m A^{m\rho} T_1^{(m)}$, e supponendo essere m l'ordine di D sarà $B = A^{m\rho} T_1^{(m)}$.

Affinchè un'espressione della forma

$$S = [x, x', \dots \quad x + p\,(ax + bx' + \dots), \quad x' + p\,(a'x + b'x' + \dots), \dots] \pmod m$$

rappresentasse una sostituzione è necessario che il determinante

$$\begin{vmatrix} 1+pa, & pb & ,\dots \\ pa' & , \; 1+pb', & \dots \\ \dots & \dots & \dots \end{vmatrix} = 1 + p^n \begin{vmatrix} a & b & \dots \\ a' & b' & \dots \\ \dots & \dots & \dots \end{vmatrix}$$

fosse primo con m, ma esso è primo con p, dunque lo dovrà essere con q. Ora, essendo p e q due numeri primi tra loro, possiamo determinare due numeri interi r ed r' tali che si abbia

$$rp + r'q = 1,$$

ed allora si può scrivere S nel seguente modo

$$S = [x, x', \dots \quad r'qx + p\,[(a+r)\,x + bx' + \dots], \quad r'qx' + p\,[a'x + (b'+r)\,x' + \dots], \dots] \pmod m$$

ed il suo determinante prenderà la seguente forma

$$\begin{vmatrix} r'q + p\,(a+r) & pb & \dots \\ pa' & r'q + p\,(b'+r)\dots \\ \dots & \dots & \dots \end{vmatrix} = (r'q)^n + p^n \begin{vmatrix} a+r & b & \dots \\ a' & b'+r\dots \\ \dots & \dots & \dots \end{vmatrix},$$

quindi perchè S possa rappresentare una sostituzione è necessario che il determinante

$$\begin{vmatrix} a+r & b & \dots \\ a' & b'+r\dots \\ \dots & \dots & \dots \end{vmatrix}$$

sia primo con q, ma questo si ottiene per $\Omega(q^n)$ sistemi di valori di $a+r$, b, etc. a cui corrispondono altrettanti sistemi di valori di a, b, etc., dunque $\Omega(q^n)$ indicherà l'ordine del gruppo H formato dalle sostituzioni della forma S.

Similmente si dimostrerebbe che $\Omega(p^n)$ sia l'ordine del gruppo H' formato dalle sostituzioni della forma

$$S' = [x, x', \dots \quad x + q\,(a_1 x + b_1 x' + \dots), \quad x' + q\,(a_1' x + b_1' x' + \dots), \dots] \pmod m$$

129. Le sostituzioni di H sono mutabili con quelle di H', poichè essendo

$$pq \equiv 0 \pmod m$$

sarà

$$SS' = S'S = \begin{vmatrix} x & x + p\,(a\,x + b\,x' + \dots) + q\,(a_1 x + b_1 x' + \dots) \\ x' & x' + p\,(a'x + b'x' + \dots) + q\,(a_1'x + b_1'x' + \dots) \\ \dots & \dots \end{vmatrix}.$$

130. Inoltre se indichiamo con S_1, S_2, S_3 etc. le sostituzioni di H e con S_1', S_2', S_3' etc. quelle di H', le altre della forma $S_r S_s'$ saranno tutte distinte. Infatti se fosse

$$S_r S_s' = S_{r'} S_{s'}',$$

sarebbe anche

$$S_{r'}^{-1} S_r = S'_{s'} S_s'^{-1},$$

e quindi $S_{r'}^{-1} S_r$ sarebbe una sostituzione comune ad H e ad H', ma le sostituzioni

comuni a questi gruppi, dovendo essere della forma

$$[x, x', \dots \;\; x + pq\,(ax + bx' + \dots), \;\; x' + pq\,(a'x + b'x' + \dots)],$$

sono uguali ad 1, dunque sarà

$$S_{r'}^{-1} S_r = 1, \quad S'_{s'} S'^{-1}_{s} = 1$$

donde
$$S_r = S_{r'}, \quad S'_s = S'_{s'}.$$

Di qui risulta che il numero delle sostituzioni $S_r S'_s$ è uguale ad

$$\Omega(p^n)\,\Omega(q^n) = \Omega(m^n),$$

ma questo è il numero delle sostituzioni del gruppo lineare G di grado m^n, dunque tutte le sostituzioni di G sono della forma $S_r S'_s$.

131. Or se y, y', etc. sono degl'indici variabili da 0 a $q-1$ ed in numero eguale agli altri x, x', etc., le sostituzioni della forma

$$\Sigma = [y, y', \dots \;\; p\,[(a+r)\,y + by' + \dots], \;\; p\,[a'y + (b'+r)\,y' + \dots], \dots] \pmod q$$

formano un gruppo I isoformo ad H. Infatti ciascuna sostituzione Σ corrisponde ad una sostituzione

$$S = [x, x', \dots \;\; r'qx + p\,[(a+r)x + bx' + \dots], \;\; r'qx' + [a'x + (b'+r)x' + \dots], \dots] \pmod m,$$

ed inoltre in forza delle relazioni

$$pq \equiv 0 \pmod m, \quad r'q \cdot r'q \equiv r'q\,(1 - rp) \equiv r'q \pmod m$$

al prodotto di due sostituzioni Σ corrisponde quello delle corrispondenti di H.

132. Posti questi principii passiamo a dimostrare la seguente proposizione.

I fattori di composizione di G sono gli uni uguali a quelli di I e gli altri a quelli di H'.

Supponiamo che I si possa scomporre nei gruppi

$$I, \;\; I', \;\; I'', \dots\dots 1 \tag{3}$$

tali che ciascuno sia contenuto nel precedente, sia permutabile alle sue sostituzioni, e sia il più generale di quelli che godono questa doppia proprietà. Siano

$$\frac{\Omega(q^n)}{f}, \quad \frac{\Omega(q^n)}{ff'}, \dots\dots$$

gli ordini di I', I'', etc.: H_1, H_2 etc. i gruppi formati dalle sostituzioni di H che corrispondono a quelle di I che formano rispettivamente I', I'' etc.; ed in fine L, L' etc. i gruppi formati moltiplicando le sostituzioni di H_1, H_2 etc. per quelle di H'.

I gruppi
$$G, \;\; L, \;\; L', \dots\dots H'$$
sono nelle stesse condizioni di quelli che formano la serie (3).

Consideriamo i due gruppi L ed L' ed indichiamo con $S_\mu S_\mu'$ una sostituzione del 1° e con $S_r S_r'$ un'altra del 2°. La trasformata di $S_r S_r'$ per mezzo di $S_\mu S_\mu'$ è appunto

$$(S_\mu S_\mu')^{-1} S_r S_r' S_\mu S_\mu',$$

ma poichè una sostituzione di H è mutabile con un'altra di H', possiamo porre la precedente sostituzione sotto la seguente forma

$$S_\mu^{-1} S_r S_\mu S'^{-1}_\mu S_r' S_\mu'.$$

Ora le sostituzioni di I che corrispondono ad S_μ^{-1}, S_r, S_μ sono rispettivamente Σ_μ^{-1}, Σ_r, Σ_μ, ma appartenendo la 1ª e la 3ª di queste ad I', e la 2ª a I'' la sostituzione $\Sigma_\mu^{-1}\Sigma_r\Sigma_\mu$ fa parte di I'', dunque la corrispondente $S_\mu^{-1}S_rS_\mu$ di H deve appartenere ad I', ma anche l'altra $S'^{-1}_\mu S'_r S'_\mu$ appartiene ad I', dunque la trasformata in parola appartiene ad L', e perciò il gruppo L', evidentemente contenuto in L, è permutabile alle sostituzioni di L.

Inoltre non vi può essere un gruppo intermedio a L ed L' che fosse permutabile alle sostituzioni di L, perchè se vi fosse vi dovrebbe essere un gruppo intermedio ad I ed I' che fosse permutabile alle sostituzioni di I, il che è contro l'ipotesi.

Ma gli ordini dei gruppi

$$G,\quad L,\quad L',\ \ldots\ldots H'$$

sono
$$\Omega(p^n)\,\Omega(q^n),\quad \Omega(p^n)\frac{\Omega(q^n)}{f},\quad \Omega(p^n)\frac{\Omega(q^n)}{ff'},\ \ldots\ \Omega(p^n)$$

ovvero
$$\Omega(m^n),\quad \frac{\Omega(m^n)}{f},\quad \frac{\Omega(m^n)}{ff'},\ \ldots\ \Omega(p^n),$$

dunque i fattori di composizione di G sono f, f', etc. e quelli di H'.

Similmente si dimostrerebbe che i fattori di composizione di H' sono gli uni uguali a quelli del gruppo lineare di grado $(\beta^\mu)^n$ e gli altri a quelli del gruppo di grado $(\gamma^r\ldots)^n$, e così di seguito.

CAPO 5.°

Forma canonica delle sostituzioni lineari.

133. Sia

$$A = |x, x', x'', \ldots\quad ax + bx' + \ldots,\quad a'x + b'x' + \ldots,\quad a''x + b''x' + \ldots, \ldots|\ (\text{mod}\, p)$$

una sostituzione del gruppo lineare di grado p^n nella quale gl'indici $x, x', x'', \ldots$ e le costanti a, b, etc. sono variabili da 0 a $p-1$. Ci proponiamo di mettere questa sostituzione sotto una forma più semplice

A tal fine osserviamo che la funzione

$$y = \alpha x + \beta x' + \gamma x'' + \ldots$$

è trasformata dalla sostituzione A nell'altra

$$\alpha(ax + bx' + \ldots) + \beta(a'x + b'x' + \ldots) + \gamma(a''x + b''x' + \ldots) + \ldots$$

la quale si riduce a Ky se α, β, γ etc. sodisfano alle relazioni

$$a\alpha + a'\beta + a''\gamma + \ldots \equiv K\alpha,\quad b\alpha + b'\beta + b''\gamma + \ldots \equiv K\beta,\ \ldots\ (\text{mod}\, p), \qquad (1)$$

essendo K una radice della congruenza

$$\Delta = \begin{vmatrix} a-K & a' & \ldots \\ b & b'-K & \ldots \\ \ldots & \ldots & \ldots \end{vmatrix} \equiv 0\ (\text{mod}\, p)$$

che chiameremo *congruenza caratteristica* di A.

Sostituendo nelle (1) successivamente le n radici $K_0, K_1, K_2 \ldots K_{n-1}$ della congruenza caratteristica si avrebbero n sistemi di congruenze da cui si potrebbero ricavare i valori del rapporti di α, β, γ, etc. corrispondenti alle indicate radici.

134. Or possiamo distinguere due casi:

1° Caso. Per ciascuna delle indicate radici si hanno pei rapporti di α, β, γ etc. dei valori determinati. Allora indicando con $\alpha_0, \beta_0, \gamma_0, \ldots : \alpha_1, \beta_1, \gamma_1, \ldots ; \ldots$ i valori di $\alpha, \beta, \gamma, \ldots$ corrispondenti rispettivamente a K_0, K_1 etc. si avranno le n funzioni

$$y_0 = \alpha_0 x + \beta_0 x' + \gamma_0 x'' + \ldots, \quad y_1 = \alpha_1 x + \beta_1 x' + \gamma_1 x'' + \ldots, \ldots$$

le quali per A sarebbero moltiplicate rispettivamente per K_0, K_1 etc. Ma sono tra loro distinte, cioè non sono tra loro legate con relazioni di 1° grado per rispetto ad esse, perchè altrimenti gl' indici x, x', x'' etc. di cui y_0, y_1 etc. sono funzioni sarebbero legate con relazioni lineari e non sarebbero più tra loro indipendenti, il che non è. Quindi possiamo sostituire agl' indici x, x' etc. gli altri y_0, y_1 etc., ed allora A prenderà la forma semplicissima

$$[y_0, y_1, \ldots K_0 y_0, K_1 y_1, \ldots].$$

135. 2° Caso. Per K_0 si hanno pei rapporti delle quantità α, β, γ, etc. dei valori indeterminati. Allora si avrebbe un numero indeterminato di funzioni le quali sarebbero moltiplicate per K_0 dalla sostituzione A. Ma tra queste necessariamente vi debbono essere delle distinte tra loro di cui tutte l'altre sono funzioni. Indichiamo con y_0, y_0', y_0'' etc. queste funzioni distinte, le quali evidentemente sono delle funzioni degl' indici primitivi x, x' etc. i cui coefficienti sono funzioni di K_0. Or se supponiamo che, essendo F un fattore irriducibile della congruenza caratteristica di A, siano $K_0, K_1, \ldots K_{l-1}$ le radici di

$$F \equiv 0 \pmod{p},$$

cambiando nelle funzioni y_0, y_0' etc. K_0 successivamente in $K_1 \ldots K_{l-1}$ si avranno l serie di funzioni conjugate $y_0, y_0' \ldots ; y_1, y_1', \ldots ; \ldots y_{l-1}, y'_{l-1}, \ldots\ldots$

Quelle che formano una medesima serie sono tra loro indipendenti, altrimenti non lo sarebbero y_0, y_0' etc., perchè una relazione che ha luogo per le funzioni di una serie deve reggere per le funzioni coniugate appartenenti ad una qualunque delle rimanenti serie. Quelle che appartengono a serie diverse sono altresì tra loro indipendenti: infatti supponiamo che si avesse la relazione

$$r y_1 + s y_2' + t y_3 \equiv 0$$

in cui r, s, t fossero funzioni di K_0, K_1 etc. Sostituendo K_0 in luogo di K_1 si avrà

$$r' y_0 + s' y_2' + t' y_3 \equiv 0,$$

e ponendo K_0 in luogo di K_2, si avrà

$$r'' y_1 + s'' y_0' + t'' y_3 \equiv 0,$$

e ponendo K_0 in luogo di K_3, si avrà

$$r''' y_1 + s''' y_2' + t''' y_0 \equiv 0,$$

ed eliminando tra queste 4 relazioni y_1, y_2', y_3, si avrà una relazione tra y_0 ed y_0',

il che è impossibile, perchè si è supposto che queste funzioni siano tra loro indipendenti.

Inoltre la A, moltiplicando le funzioni y_0, y_0' etc. per K_0, moltiplicherà le funzioni della serie conjugata y_ρ, y_ρ' etc. per la radice corrispondente K_ρ. Infatti se la funzione

$$\varphi = a + bK_0 + cK_0^2 + \ldots + eK_0^{l-1}$$

nella quale a, b, c etc. sono funzioni degl'indici x, x', etc. è trasformata da A nell'altra

$$\varphi_1 = a' + b'K_0 + c'K_0^2 + \ldots + e'K_0^{l-1},$$

dovranno le funzioni a, b, c etc. essere trasformate da questa sostituzione rispettivamente nell'altre a', b', c' etc., quindi la funzione

$$\varphi' = a + bK_\rho + cK_\rho^2 + \ldots + eK_\rho^{l-1}$$

conjugata di φ dovrà essere trasformata nell'altra

$$\varphi_1' = a' + b'K_\rho + c'K_\rho^2 + \ldots + e'K_\rho^{l-1}$$

conjugata di φ'.

Da quanto si è detto risulta che si possano prendere per indici le funzioni delle indicate l serie in luogo di altrettanti indici primitivi; ed allora la sostituzione A prenderà la seguente forma.

$$A = \left| \begin{array}{ll} y_0 & K_0 y_0 \\ y_0' & K_0 y_0' \\ \vdots & \vdots \\ y_1 & K_1 y_1 \\ \vdots & \vdots \\ x^m & a_1^m x^m + b_1^m x^{m+1} + \ldots + f(y_0, y_0' \ldots y_1 \ldots) \\ \vdots & \vdots \\ x^{n-1} & a_1^{n-1} x^m + b_1 x^{m+1} + \ldots + f_r(y_0, y_0' \ldots y_1 \ldots) \end{array} \right|$$

e la sua congruenza caratteristica prenderà la forma

$$(K - K_0)^\lambda (K - K_1)^\lambda \ldots \left| \begin{array}{ll} a_1^m - K, & b_1^m \ldots\ldots\ldots \\ a_1^{m+1} \quad , & b_1^{m+1} - K \ldots \\ \ldots\ldots\ldots & \ldots\ldots\ldots \end{array} \right| \equiv 0 \pmod{p},$$

essendo λ il numero delle funzioni y_0, y_0' etc.

136. Ma la caratteristica di una sostituzione non si altera per un cambiamento d'indici, quindi Δ dovrà essere divisibile per

$$(K - K_0)^\lambda (K - K_1)^\lambda \ldots,$$

ossia per la potenza λ^{ma} del fattore F di Δ; e siccome F^λ è un polinomio a coefficienti reali, il quoziente di questa divisione

$$\Delta' = \begin{vmatrix} a_1^m - K & b_1^m & \dots c_1^m \\ a_1^{m+1} & b_1^{m+1} - K \dots & c_1^{m+1} \\ \dots\dots & \dots\dots & \dots\dots \\ a_1^{n-1} & b_1^{n-1} & \dots c_1^{n-1} - K \end{vmatrix}$$

sarà anche un polinomio in K a coefficienti reali.

Sia F' un fattore irriducibile di Δ' e $K_0', K_1', \dots K'_{r-1}$ le radici di $F' = 0$. La sostituzione

$$\begin{vmatrix} x^m & a_1^m x^m + b_1^m x^{m+1} + \dots + c_1^m x^{n-1} \\ x^{m+1} & a_1^{m+1} x^m + b_1^{m+1} x^{m+1} + \dots + c_1^{m+1} x^{n-1} \\ \dots\dots & \dots\dots\dots\dots \\ x^{n-1} & a_1^{n-1} x^m + b_1^{n-1} x^{m+1} + \dots + c_1^{n-1} x^{n-1} \end{vmatrix}$$

si potrà porre sotto la forma

$$\begin{vmatrix} z_0 & K_0' z_0 \\ z'_0 & K_0' z_0' \\ \vdots & \vdots \\ z_1 & K_1' z' \\ \vdots & \vdots \\ x^{m+m'} & a_2^{m+m'} x^{m+m'} + b_2^{m+m'} x^{m+m'+1} + \dots + c_2^{m+m'} x^{n-1} \\ \vdots & \vdots \\ x^{n-1} & a_2^{n-1} x^{m+m'} + b_2^{n-1} x^{m+m'+1} + \dots + c_2^{n-1} x^{n-1} \end{vmatrix}.$$

Quindi facendo questo cambiamento d'indici nella precedente trasformata di A. si avrà la nuova trasformata

$$A = \begin{vmatrix} y_0 & K_0 y_0 \\ y_0' & K_0 y_0' \\ \vdots & \vdots \\ y_1 & K_1 y_1 \\ \vdots & \vdots \\ z_0 & K_1' z_0 + f(y_0 y_0' \dots y_1 \dots) \\ z_0' & K_0' z_0' + f_1(y_0 y_0' \dots y_1 \dots) \\ \vdots & \vdots \\ z_1 & K_1' z_1 + f_r(y_0 y_0' \dots y_1 \dots) \\ \vdots & \vdots \\ x^{m+m'} & a_2^{m+m'} x^{m+m'} + \dots + c_2^{m+m'} x^{n-1} + f_1(y_0 . y_0' \dots y_1 \dots z_0 . z_0' \dots z_1 \dots) \\ \dots\dots & \dots\dots\dots\dots \\ x^{n-1} & a_2^{n-1} x^{m+m'} + \dots + c_2^{n-1} x^{n-1} + f_n(y_0 . y_0' \dots y_1 \dots z_0 . z_0' \dots z_1 \dots) \end{vmatrix}.$$

Facendo il cambiamento d'indici diretto a semplificare la sostituzione

$$\begin{vmatrix} x^{m+m'} & a_2^{m+m'} x^{m+m'} + \dots + c_2^{m+m'} x^{n-1} \\ \dots\dots & \dots\dots\dots\dots \\ x^{n-1} & a_2^{n-1}\; x^{m+m'} + \dots + c_2^{n-1}\; x^{n-1} \end{vmatrix}.$$

e così seguitando, si giungerà a dare ad A la seguente forma

$$A = \begin{vmatrix} y_0\,,\, y_0'\,,\, \dots\dots\; K_0 y_0\,,\, K_0 y_0'\,,\, \dots\dots\dots\dots \\ y_1\,,\, y_1'\,,\, \dots\dots\; K_1 y_1\,,\, K_1 y_1'\,,\, \dots\dots\dots\dots \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ z_0\,,\, \dots\dots\dots\dots\; K_0'\, z_0 + \varphi\,(y_0\,,\, y_0' \dots y_1\,,\, y_1' \dots) \\ z_1\,,\, \dots\dots\dots\dots\; K_1'\, z_1 + \varphi_1(y_0\,,\, y_0' \dots y_1\,,\, y_1' \dots) \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ u_0\,,\, \dots\dots\dots\dots\; K_0''\, u_0 + \psi\,(y_0\,,\, y_0' \dots y_1\,,\, y_1' \dots z_0 \dots z_1 \dots) \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ v_0\,,\, \dots\dots\dots\dots\; K_0''' v_0 + \chi\,(y_0\,,\, y_0' \dots y_1\,,\, y_1' \dots z_0 \dots z_1 \dots u_0) \end{vmatrix}$$

nella quale si sono posti in linea orizzontale tutti gl'indici che si riferiscono ad una stessa radice di $\Delta \equiv 0$.

137. Supponiamo che i fattori irriducibili F', F'' di Δ a cui corrispondono rispettivamente le radici K_0', K_0'' siano uguali ad F, e che l'altro F''' a cui appartiene la radice K_0''' sia diverso da F, allora sarà $K_0 = K_0' = K_0''$ e K_0''' sarà diversa da K_0.

Ora la funzione

$$w_0 = v_0 + \rho_0 u_0 + \dots + \sigma_0 z_0 + \dots + \sigma_1 z_1 + \dots + \theta_0 y_0 + \theta_0' y_0' + \dots + \theta_1 y_1 + \dots$$

è trasformata dalla sostituzione A nell'altra

$$K_0''' w_0 + \chi'\,(y_0\,,\, y_0' \dots y_1 \dots z_0 \dots z_1 \dots\; u_0 \dots)$$

ed i coefficienti di $u_0 \dots z_0 \dots z_1 \dots y_0\,,\, y_0' \dots y_1 \dots$ in χ' hanno rispettivamente la forma

$$(K_0 - K_0''')\,\rho_0 + a\,, \quad (K_1 - K_0''')\,\sigma_0 + b\rho_0 + c\,, \quad (K_1 - K_0''')\,\sigma_1 + d\rho_1 + e\,, \dots$$

l'guagliando a 0 (mod p) questi coefficienti si avranno delle congruenze dalle quali si potranoo sempre dedurre dei valori determinati per $\rho_0\,,\, \sigma_0\,,\, \dots$; e sostituendo questi valori nell'espressione di w_0, si avrà un valore di w_0 che sarà moltiplicato da K_0''' dalla sostituzione A.

Il valore di w_0 così determinato non conterrà altro immaginario che K_0'''. Invero se si incominciasse la semplificazione di A dall'adoperare le radici K_0''' etc. del fattore irriducibile F''' si dovrebbero avere degl'indici, funzioni di K_0''', i quali sarebbero moltiplicati da A per K_0''', ma A moltiplica w_0 per K_0''', quindi w_0 dovrà essere funzione dei soli sopra indicati indici e per conseguenza dovrà essere w_0 funzione del solo immaginario K_0'''.

Sostituendo nell'ultima trasformata di A all'indice v_0 l'altro w_0 ed ai rimanenti che appartengono al fattore F'' di Δ delle funzioni determinate come w_0, cioè delle funzioni delle radici di $F''' \equiv 0$ (mod p) indipendenti dagl'indici $y_0\,,\, y_0' \dots y_1 \dots z_0 \dots u_0 \dots$

appartenenti al fattore F di Δ, e lo stesso facendo per gl'indici appartenenti agli altri fattori di Δ, la sostituzione A prenderà la seguente forma

$$A = \left| \begin{array}{l} y_0\,,\, y_0' \ldots\ldots K_0 y_0\,,\, K_0 y_0' \ldots\ldots \\ y_1\,,\, y_1' \ldots\ldots K_1 y_1\,,\, K_1 y_1' \ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ z_0 \ldots\ldots\ldots\ldots K_0 z_0 + \varphi\,(y_0\,,\, y_0' \ldots y_1 \ldots y_1' \ldots) \ldots \\ z_1 \ldots\ldots\ldots\ldots K_1 z_1 + \varphi_1(y_0\,,\, y_0' \ldots y_1 \ldots y_1' \ldots) \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ u_0 \ldots\ldots\ldots\ldots K_0 u_0 + \psi\,(y_0\,,\, y_0' \ldots y_1 \ldots y_1' \ldots) \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ w_0 \ldots\ldots\ldots\ldots K''' w_0 \ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array} \right|$$

in cui gl'indici sono divisi in sistemi tali che gl'indici di ciascun sistema sono rimpiazzati da funzioni lineari degl'indici del medesimo sistema: il 1° di questi sistemi comprende gl'indici $y_0\,,\, y_0' \ldots$; $y_1\,,\, y_1' \ldots z_0 \ldots z_1 \ldots$; $u_0 \ldots$ relativi al fattore F di Δ, il 2° gl'indici $w_0 \ldots$ relativi al fattore F''', e così di seguito.

138. Consideriamo il 1° sistema d'indici e sostituiamo agl'indici $z_0 \ldots . u_0 \ldots .$ gl'altri

$$(z_0) = z_0 + \rho y_0 + \rho' y_0' + \ldots\,, \quad (u_0) = u_0 + \sigma z_0 + \ldots + \theta y_1 + \theta' y_1' + \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

i quali da A sono mutati in

$$K_0\,(z_0) + \varphi'(y_0\,,\, y_0' \ldots y_1\,,\, y_1' \ldots)\,, \quad K_0\,(u_0) + \psi'(y_0\,,\, y_0' \ldots y_1\,,\, y_1'\,,\, z_0 \ldots z_1 \ldots)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Ma siccome i coefficienti di $y_1, y_1' \ldots z_1 \ldots$ in φ', ψ' etc. sono

$$(K_0 - K_1)\,\rho + a\,, \quad (K_0 - K_1)\,\rho' + a' \ldots$$

$$(K_0 - K_1)\,\sigma + b\,, \quad (K_0 - K_1)\,\theta + c\rho + d\,, \quad (K_0 - K_1)\,\theta' + c'\rho + d', \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

determinando le costanti ρ, ρ', etc. mediante le relazionj che risultano uguagliando a zero (mod p) le precedenti espressioni, si avranno per valori di (z_0), (u_0) etc. delle espressioni che saranno trasformate da A in altre che non conterranno $y_1\,,\, y_1' \ldots z_1 \ldots$ Inoltre (z_0), (u_0) sono funzioni degl'indici primitivi che non contengono altro immaginario che K_0; poichè K_1, a, b. c, d etc. sono funzioni di K_0 quindi $\rho, \rho', \sigma, \sigma' \ldots$ non conterranno d'immaginario che K_0.

Sostituiamo agl'indici $z_1 \ldots u_1 \ldots$ rispettivamente le funzioni $(z_1 \ldots (u_1) \ldots$ conjugate di $(z_0) \ldots (u_0) \ldots$ ed allora, togliendo le parentesi divenute inutili, la sostituzione A prenderà la forma

$$A = \left| \begin{array}{l} y_0\,,\, y_0' \ldots\ldots K_0 y_0 \quad K_0 y_0' \ldots \ldots \\ z_0\,,\, z_0' \ldots\ldots K_0 z_0 + \varphi\,(y_0\,,\, y_0' \ldots)\,, \quad K_0 z_0' + \varphi'\,(y_0\,,\, y_0' \ldots) \\ u_0,\, u_0' \ldots\ldots K_0 u_0 + \psi\,(z_0\,,\, z_0' \ldots y_0\,,\, y_0' \ldots)\,, \quad K_0 u_0' + \psi'\,(z_0\,,\, z_0' \ldots y_0\,,\, y_0' \ldots) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ y_1\,,\, y_1' \ldots\ldots K_1 y_1 \quad K_1 y_1' \ldots\ldots \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ w_0 \ldots\ldots\ldots\ldots K_0''' w_0 \ldots\ldots\ldots\ldots \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{array} \right|$$

nella quale gl'indici del 1° sistema sono divisi in l serie conjugate

$$y_0\,,\, y_0' \ldots z_0 \ldots u_0\,; \quad y_1\,,\, y_1' \ldots z_1 \ldots u_1 \ldots ; \ldots$$

corrispondenti rispettivamente alle radici K_0, K_1 etc. del fattore irriducibile F.

139. Ora le funzioni $\psi\,(z_0\,,\, z_0' \ldots y_0\,,\, y_0' \ldots)$, $\psi'(z_0\,,\, z_0' \ldots y_0\,,\, y_0' \ldots)$ sono tra loro indipendenti, perchè se fossero legate da una relazione della forma

$$r\psi + r'\psi' \ldots \equiv 0$$

gl'indici $z_0\,,\, z_0' \ldots$ non sarebbero più indipendenti fra loro, il che non è. Quindi possiamo invece di $z_0\,,\, z_0'$, etc. prendere per indici le funzioni Z_0, Z_0' determinate dalle seguenti relazioni

$$K_0 Z_0 = \psi\,(z_0 z_0' \ldots y_0\,,\, y_0' \ldots)\,, \quad K_0 Z_0' = \psi'\,(z_0 z_0' \ldots y_0 y_0' \ldots)\,, \ldots$$

ed allora A cambierà uno di questi nuovi indici per esempio Z_0 in $K_0 Z_0$ più una funzione di $y_0\,,\, y_0'$ etc.; e gl'altri $u_0\,,\, u_0'$ etc. rispettivamente in $K_0\,(u_0 + Z_0)$, $K_0\,(u_0' + Z_0')$, ...

Analogamente possiamo sostituire a tutti o ad una parte degl'indici $y_0\,,\, y_0' \ldots$ dei nuovi indici $Y_0\,,\, Y_0' \ldots$ scelti in modo che A permuti $Z_0\,,\, Z_0' \ldots$ rispettivamente in $K_0\,(Z_0 + Y_0)$, $K_0\,(Z_0' + Y_0')$, ...

Continuando questa riduzione si perverrà a porre A sotto la seguente forma

$$A = \left| \begin{array}{l} Y_0\,,\, Z_0\,,\, u_0 \ldots \; K_0 Y_0\,,\, K_0\,(Y_0 + Z_0),\, K_0\,(u_0 + Z_0) \ldots \\ Y_0',\, Z_0' \ldots\ldots\ldots \; K_0 Y_0'\,,\, K_0\,(Z_0' + Y_0') \ldots\ldots\ldots\ldots\ldots \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{array} \right|$$

nella quale gl'indici della 1ª serie si trovano divisi in serie distinte $Y_0, Z_0, u_0 \ldots$; $Y_0', Z_0' \ldots ; \ldots$ che A altera con una legge semplicissima.

Per semplificare le alterazioni che A fa subire ad un'altra serie $y_\rho, y_\rho' \ldots$ conjugata di $y_0, y_0' \ldots$ basterà cambiare gl'indici y_ρ, y_ρ' etc. negl'altri indici $Y_\rho, Z_\rho, u_\rho \ldots$, $Y_\rho', Z_\rho' \ldots ; \ldots$ conjugati di $Y_0\,,\, Z_0\,,\, u_0 \ldots$; $Y_0', Z_0' \ldots ; \ldots$ e questi nuovi indici saranno da A permutati rispettivamente in

$$K_\rho Y_\rho\,, \quad K_\rho\,(Y_\rho + Z_\rho)\,, \; K_\rho\,(u_\rho + Z_\rho) \ldots$$
$$K_\rho Y_\rho'\,, \quad K_\rho\,(Z_\rho' + Y_\rho')\,, \ldots\ldots\ldots\ldots\ldots$$

140. Da quanto si è detto si deduce il seguente

Teorema. — *Sia*

$$A = [x\,, x', \ldots \quad ax + bx' + \ldots \quad a'x + b'x' + \ldots, \ldots]$$

una sostituzione lineare qualunque a coefficienti reali tra n *indici variabili da* 0 *a* p − 1; *siano* F, F′... *i fattori irriducibili della congruenza di grado* n

$$\begin{vmatrix} a - K & a' \ldots\ldots \\ b & b' - K \ldots \\ \ldots\ldots\ldots\ldots & \end{vmatrix} \equiv 0 \pmod{p};$$

l, l′.... *i loro gradi rispettivi; ed* m, m′,.... *i loro gradi di multiplicità. Si potranno cambiare gli* n *indici indipendenti* x, x′... *in altri indici che godono le seguenti proprietà:*

1.° *Questi indici si dividono in sistemi corrispondenti ai diversi fattori* F, F′... *e contenenti rispettivamente* lm, l′m′, ... *indici;*

2.° *Siano* $K_0, K_1 \ldots K_{l-1}$ *le radici della congruenza irriducibile* $F \equiv 0 \pmod{p}$; *gli* lm *indici del sistema corrispondente ad* F *si dividono in* l *serie corrispondenti alle radici* $K_0, K_1 \ldots K_{l-1}$;

3.° *Gl' indici della 1ª serie di questo sistema sono delle funzioni lineari degl' indici primitivi, i di cui coefficienti sono funzioni di* K_0; *essi costituiscono una o più serie* $y_0, z_0, u_0 \ldots;\ y_0', z_0' \ldots;\ \ldots$ (*) *tali che* A *permuta gl' indici* $y_0, z_0, u_0, \ldots$ *d' una stessa serie rispettivamente in* $K_0 y_0,\ K_0(z_0 + y_0)\ K_0(u_0 + z_0) \ldots$;

4.° *Gl' indici della* r+1ᵐᵃ *serie saranno le funzioni* $y_r, z_r, u_r \ldots, y_r', z_r', u_r' \ldots; \ldots$ *rispettivamente conjugate delle precedenti, e che si formano ponendo* K_r *in luogo di* K_0: *la sostituzione* A *scambierà quest' indici rispettivamente coll' espressioni*

$$K_r\, y_r\,, \quad K_r(z_r + y_r), \quad K_r(u_r + z_r) \ldots; \ldots$$

Diremo forma canonica di A la seguente

$$\begin{vmatrix} y_0, z_0, u_0 \ldots;\ y_0' \ldots & K_0 y_0, & K_0(z_0 + y_0), & K_0(u_1 + z_0) \ldots; & K_0 y_0' \ldots \\ y_1, z_1, u_1 \ldots;\ y_1' \ldots & K_1 y_1, & K_1(z_1 + y_1), & K_1(u_1 + z_1) \ldots; & K_1 y_1' \ldots \\ \ldots\ldots\ldots\ldots & \ldots & \ldots & \ldots & \ldots \\ v_0 \ldots\ldots\ldots & K_0' v_0 \ldots & \ldots & \ldots & \ldots \\ \ldots\ldots\ldots\ldots & \ldots & \ldots & \ldots & \ldots \end{vmatrix}.$$

141. Questa forma ci conduce facilmente a trovare l'ordine di A.

Supponiamo che la potenza λ di A abbia la seguente forma

$$\begin{vmatrix} y_0, z_0, u_0 \ldots;\ y_0' \ldots & K_0^{\lambda} y_0, & K_0^{\lambda}(z_0 + \lambda y_0), & K_0^{\lambda}\left[u_0 + \lambda z_0 + \frac{\lambda(\lambda-1)}{2} y_0\right] \ldots & \lambda_0 y_0' \ldots \\ y_1, z_1, u_1 \ldots;\ y_1' \ldots & K_1^{\lambda} y_1, & K_1^{\lambda}(z_1 + \lambda y_1), & K_1^{\lambda}\left[u_1 + \lambda z_1 + \frac{\lambda(\lambda-1)}{2} y_1\right] \ldots & \lambda_1 y_1' \ldots \\ \ldots\ldots\ldots\ldots & \ldots & \ldots & \ldots & \ldots \\ v_0 \ldots\ldots\ldots & \lambda_0' v_0 \ldots & \ldots & \ldots & \ldots \\ \ldots\ldots\ldots\ldots & \ldots & \ldots & \ldots & \ldots \end{vmatrix}$$

(*) Qui si dinotano con $y_0, z_0 \ldots$ gli indici che sono stati dinotati prima con $Y_0, Z_0, \ldots$

e che siano $$K_0^\lambda\left[w_0+\lambda v_0+\ldots+\frac{\lambda(\lambda-1)\ldots(\lambda-r+1)}{r!}y_0\right]$$

$$K_0^\lambda\left[X_0+\ldots+\frac{\lambda(\lambda-1)\ldots(\lambda-r+2)}{(r-1)!}y_0\right]$$

l'espressioni con cui A^λ scambia rispettivamente gl'indici $r+1^{mo}$ ed r^{mo} della serie $y_0, z_0, u_0 \ldots$

Per avere la funzione che $A^{\lambda+1}$ pone in luogo del $r+1^{mo}$ indice dell'indicata serie bisogna addizionare le soprascritte espressioni dopo averle moltiplicate per K_0; ma la somma dei coefficienti dei termini $r+1^{mo}$ ed r^{mo} dello sviluppo di $(x+a)^\lambda$ dà il coefficiente del termine $r+1^{mo}$ dello sviluppo di $(x+a)^{\lambda+1}$, dunque l'indicata somma sarà

$$K_0^{\lambda+1}\left[w_0+(\lambda+1)X_0+\ldots+\frac{(\lambda+1)\lambda\ldots(\lambda-r+2)}{r!}y_0\right],$$

per conseguenza se la legge si verifica per la potenza λ^{ma} di A si verificherà anche per la $\lambda+1^{ma}$, ma essa si verifica per la 2^a, adunque la legge è generale

Se λ è l'ordine di A è necessario che abbiano luogo le relazioni

$$(1)\qquad K_0^\lambda\equiv K_1^\lambda\equiv\ldots\equiv 1,\quad K_0^\lambda\lambda\equiv 0,\quad K_0^\lambda\frac{\lambda(\lambda-1)}{2}\equiv 0\ldots K_0'^\lambda\equiv 1\ldots \pmod p$$

per modo che se ρ indica il numero degl'indici contenuti nella più lunga delle serie $y_0, z_0, \ldots;\ y_0', z_0'\ldots;\ldots$ dovrà essere

$$(2)\qquad \lambda\equiv 0,\quad \frac{\lambda(\lambda-1)}{2}\equiv 0,\ldots\frac{\lambda(\lambda-1)\ldots(\lambda-\rho+2)}{(\rho-1)!}\equiv 0 \pmod p.$$

La 1^a di queste congruenze esprime che λ debba essere divisibile per p. Or se dinotiamo con p^α la massima potenza di p contenuta in λ e con p^q la massima potenza di p inferiore a ρ è necessario che fosse $\alpha > q+1$ affinchè le (2) abbiano luogo. Infatti se fosse altrimenti tra le (2) vi sarebbe la congruenza

$$\frac{\lambda(\lambda-1)\ldots(\lambda-p^\alpha+1)}{1\cdot 2\ldots p^\alpha}\equiv 0 \pmod p$$

la quale non potrebbe aver luogo; perchè $\lambda-1,\ \lambda-2,\ldots\lambda-p^\alpha+1,\ \lambda$ conterrebbero rispettivamente le stesse potenze di p che si contengono in $1, 2,\ldots, p^\alpha-1, p^\alpha$, quindi il 1° membro della congruenza non sarebbe divisibile per p.

Ora è sufficiente che fosse $\alpha=q+1$ perchè avessero luogo le (3). Infatti sia

$$\frac{\lambda(\lambda-1)\ldots(\lambda-r+1)}{r!}\equiv 0$$

una di esse. Essendo $r<p^{q+1}$, $\lambda-1,\ldots\lambda-r+1$ sono rispettivamente divisibili per quelle potenze di p che dividono $1, 2\ldots r-1$, ma r contiene una potenza di p minore di p^{q+1}, dunque la precedente congruenza è soddisfatta.

Inoltre affinchè λ sia l'ordine di A è necessario che avessero luogo le relazioni

$$K_0^\lambda\equiv K_1^\lambda\equiv\ldots\equiv 1,\quad K_0'^\lambda\equiv 1\ldots \pmod p,$$

quindi λ dovrà essere divisibile per gl'esponenti $\delta_0, \delta_1\ldots\delta'\ldots$ delle più piccole po-

tenze di $K_0, K_1 \ldots, K_0' \ldots$ che sono congrue ad 1, e per conseguenza dovrà essere divisibile pel loro minimo multiplo d.

Or se $\nu_0, \nu_1 \ldots; \nu' \ldots$ sono rispettivamente i gradi degl'immaginarii $K_0, K_1 \ldots; K_0' \ldots$ i numeri $\delta_0 \delta_1 \ldots; \delta' \ldots$ debbono rispettivamente dividere $p^{\nu} - 1$, $p^{\nu_1} - 1, \ldots; p^{\nu'} - 1 \ldots$, ma se μ è il più piccolo multiplo di $\nu_0, \nu_1 \ldots; \nu' \ldots$, $p^{\mu} - 1$ è divisibile per $p^{\nu_0} - 1$, $p^{\nu_1} - 1 \ldots; p^{\nu'} - 1 \ldots$, adunque anche $\delta_0, \delta_1, \ldots, \delta' \ldots$ ed il loro minimo multiplo d dovranno dividere $p^{\mu} - 1$, ma $p^{\mu} - 1$ è primo con p, adunque anche d è primo con p.

Dovendo λ essere divisibile per i due numeri d e p^{q+1} che sono primi tra loro, sarà divisibile pel loro prodotto dp^{q+1}; ma questo numero soddisfa a tutte le condizioni (1), dunque esso è il più piccolo valore di λ per cui si abbia $A^{\lambda} \equiv 1$, e perciò rappresenta l'ordine di A.

142. Corollario. — Se l'ordine di A è uguale a p, sarà $K_0^{p} \equiv 1$, donde $K_0^{p^{\nu_0}} \equiv 1$, ma si ha $K_0^{p^{\nu_0}-1} \equiv 1$, dunque $K_0 \equiv K_0^{p^{\nu_0}} \equiv 1$. Similmente si ha $K_1 \equiv 1 \ldots K_0' \equiv 1 \ldots$ Dunque la congruenza caratteristica di ogni sostituzione lineare di ordine p ha le sue radici uguali ad 1, e perciò può essere ridotta alla sua forma canonica con una trasformazione d'indici reali.

Se la sostituzione A si riducesse alla forma

$$(y_0, y_0' \ldots, y_0, y_1' \ldots \nu_0 \ldots K_0 y_0, K_0 y_0' \ldots K_1 y_1, K_1 y_1' \ldots K_0' \nu_0 \ldots)$$

le (1) si ridurrebbero all'altre

$$K_0^{\lambda} \equiv K_1^{\lambda} \equiv \ldots \equiv 1, \quad K_0' \equiv 1 \ldots$$

e λ si ridurrebbe a $d \ldots$

CAPO 7.°

Sostituzioni mutabili con una data sostituzione.

143. Teorema 1.° — *Sia A una sostituzione ridotta alla sua forma canonica e B un'altra sostituzione riferita agli stessi indici di A e che scambia gl'indici di una serie con funzioni lineari degl'indici della stessa serie, affinchè B sia reale è necessario e sufficiente che a ciascuno degl'indici di una serie sostituisca una funzione di quest'indici i cui coefficienti non contengano altro immaginario che la radice corrispondente a questa serie.*

Supponiamo che indicando con K_0, K_1 due radici di un medesimo fattore irriducibile della congruenza caratteristica di A e con K' una radice di un altro fattore della stessa congruenza, si abbia

$$A = [y_0, z_0, y_1, z_1, v \quad K_0 y_0, K_0(y_0 + z_0), K_1 y_1, K_1(y_1 + z_1), K'v]$$

$$B = [y_0, z_0, y_1, z_1 \quad a_0 y_0 + b_0 z_0, a_0' y_0 + b_0' z_0, a_1 y_1 + b_1 z_1, a_1' y_1 + b_1' z_1].$$

Supponiamo inoltre che sia

$$y_0 = Y_0 + K_0 Y_1, \quad z_0 = Z_0 + K_0 Z_1, \quad y_1 = Y_0 + K_1 Y_1, \quad z_0 = Z_0 + K_1 Z_1.$$

indicando Y_0, Y_1, Z_0, Z_1 delle funzioni reali degli indici reali a cui era riferita A prima di essere ridotta alla sua forma canonica.

Risolvendo le precedenti equazioni per rispetto ad Y_0, Z_0, Y_1, Z_1 si avranno per queste quantità dei valori che saranno tra loro indipendenti, altrimenti non

lo sarebbero y_0, z_0, y_1, z_1, quindi possiamo trasformare B cambiando gl'indici z_0, z_0, y_1, z_1 negli altri Y_0, Z_0, Y_1, Z_1. Allora perchè la B fosse reale sarebbe necessario che permutasse ciascuno degl'indici Y_0, Z_0, Y_1, Z_1 con funzioni reali dei medesimi indici, quindi ad y_0 ed a z_0 dovrebbo sostituire delle quantità che non contenessero altro immaginario che K_0, ma essa sostituisce $a_0y_0+b_0z_0$, $a_0'y_0+b_0'z_0$ rispettivamente ad y_0 e a z_0, dunque se in queste espressioni poniamo in luogo di y_0 e di z_0 i loro valori i quali non contengono altro immaginario che K_0 si debbono avere dei risultati che non contengano altro immaginario che K_0, il che richiede che a_0, b_0, a_0', b_0' non contengano altro immaginario che K_0, ma $a_1y_1+b_1z_1$, $a_1'y_1+b'z_1$ sono rispettivamente conjugati di $a_0y_0+b_0z_0$, $a_0'y_0+b_0'z_0$, quindi a_1, b_1, a_1', b_1' non debbono contenere altro immaginario che K_1, e perciò la condizione indicata è necessaria.

Inoltre essa è sufficiente, poichè supponendo che si abbia

$$a_0y_0+b_0z_0=(Y)+(Y_1)K_0,\quad a_1y_1+b_1z_1=(Y)+(Y_1)K_1,$$

per essere
$$y_0=Y_0+Y_1K_0,\quad y_1=Y_0+Y_1K_1$$

la sostituzione B scambierà Y_0 ed Y_1 rispettivamente colle funzioni reali (Y), (Y_1), come anche permuterà Z e Z_1 con funzioni reali, quindi B sarà reale.

144. Teorema 2.° — *Affinchè una sostituzione B sia mutabile con un'altra A ridotta alla sua forma canonica è necessario che scambi gl'indici di una serie con funzioni lineari degl'indici della stessa serie.*

Supponiamo che A abbia la forma prima indicata, e B l'altra

$$B=[y_0, z_0, y_1\ldots\quad ay_0+bz_0+cy_1+dz_1+ev,\quad a'y_0+b'z_0+\ldots,\quad a''y_0+\ldots,\ldots].$$

Affinchè A sia mutabile con B è necessario che le due operazioni AB e BA producano per ciascun indice la stessa alterazione, quindi dovrà essere

$$aK_0y_0+bK_0(z_0+y_0)+cK_1y_1+dK_1(z_1+y_1)+eK'v$$
$$\equiv K_0(ay_0+bz_0+cy_1+dz_1+ev)$$
$$a'K_0y_0+b'K_0(z_0+y_0)+c'K_1y_1+d'K_1(z_1+y_1)+e'K'v$$
$$\equiv K_0(a'y_0+b'z_0+c'y_1+d'z_1+e'v+ay_0+bz_0+cy_1+dz_1+ev)$$

....

Uguagliando i coefficienti di ciascun indice nei due membri di ciascuna di queste relazioni, si hanno oltre delle altre relazioni le seguenti

$$eK'\equiv K_0e\qquad dK_1\equiv K_0d\qquad cK_1+dK_1\equiv K_0c$$
$$e'K'\equiv K_0e'+K_0e\quad d'K_1\equiv K_0d'+K_0d\quad c'K_1+d'K_1\equiv K_0c'+K_0c,$$

e poichè K_0 non è congruo a K_1 dovrà essere

$$c\equiv 0,\quad d\equiv 0,\quad e\equiv 0,\quad d'\equiv 0,\quad e'\equiv 0.$$

145. Corollario 1.° — Come una sostituzione A ridotta alla sua forma canonica può scomporsi in altre sostituzioni A_1, A_2 etc. ciascuna delle quali opera su gl'indici di un medesimo sistema, così una sostituzione B mutabile ad A può scomporsi in altre B_1, B_2 etc. ciascuna delle quali opera sopra gl'indici dello stesso

sistema. Di qui risulta: 1° che per essere B reale è necessario che lo sia ciascuna dell'altre B_1, B_2 etc.: 2° che per essere B mutabile ad A debbano essere A_1, A_2 etc. rispettivamente mutabili con B_1, B_2 etc.

146. Corollario 2.° — Come A_1 può scomporsi in altre sostituzioni $A_1^{(1)}$, $A_1^{(2)}$ etc. ciascuna delle quali opera sopra gl'indici di una medesima serie, così B_1 può scomporsi in altre sostituzioni $B_1^{(1)}$, $B_1^{(2)}$ etc. ciascuna delle quali opera sopra gl'indici di una medesima serie. E poichè $A_1^{(2)}$, $A_1^{(3)}$ etc. $B_1^{(2)}$, $B_1^{(3)}$ etc. si ottengono rispettivamente da $A_1^{(1)}$ e $B_1^{(1)}$ scambiando K_0 in K_1, K_2 etc., così se le operazioni $A_1^{(1)} B_1^{(1)}$, $B_1^{(1)} A_1^{(1)}$ sono identiche, le operazioni $A_1^{(2)} B_1^{(2)}$, $A_1^{(3)} B_1^{(3)}$ etc. saranno rispettivamente identiche all'altre $B_1^{(2)} A_1^{(2)}$, $B_1^{(2)} A_1^{(3)}$ etc.; ma per essere A_1 mutabile a B_1 deve essere $A_1^{(1)} B_1^{(1)} = B_1^{(1)} A_1^{(1)}$, dunque la condizione necessaria e sufficiente perchè A_1 sia mutabile a B_1 è che $A_1^{(1)}$ lo sia a $B_1^{(1)}$, lo stesso è da dirsi di A_2 e B_2, di A_3 e B_3 etc.

147. Corollario 3.° — Se l'operazione

$$B_1^{(1)} = [y_0,\ z_0 \quad a_0 y_0 + b_0 z_0,\quad a_0' y_0 + b_0' z_0]$$

è una sostituzione il suo determinante $\begin{vmatrix} a_0 & b_0 \\ a_0' & b_0' \end{vmatrix}$ è diverso da zero. Ora quello di una qualunque delle operazioni $B_1^{(2)}$, $B_1^{(3)}$... per esempio di $B_1^{(n)}$ si ottiene scambiando in $\begin{vmatrix} a_0 & b_0 \\ a_0' & b_0' \end{vmatrix}$ K_0 nella radice K_{n-1} corrispondente a $B_1^{(n)}$, ma questa radice è congrua alla potenza $K_0^{p^{n-1}}$ la quale sostituita nel precedente determinante dà un risultato che differisce per un multiplo di p da $\begin{vmatrix} a_0 & b_0 \\ a_0' & b_0' \end{vmatrix}^{p^{n-1}}$, quindi il determinante di $B_1^{(n)}$ sarà diverso da zero, epperò $B_1^{(n)}$ rappresenterà una sostituzione.

Inoltre se $B_1^{(1)}$ è una sostituzione reale a_0, b_0, a_0', b_0' non conterranno altro immaginario che K_0, e quindi i coefficienti di $B_1^{(n)}$ non conterranno altro immaginario che K_{n-1} e sarà perciò $B_1^{(n)}$ una sostituzione reale.

Laonde la ricerca delle sostituzioni reali B mutabili ad A si riduce a quella delle sostituzioni reali $B_1^{(1)}$, $B_2^{(1)}$, $B_3^{(1)}$ etc. rispettivamente mutabili all'altre $A_1^{(1)}$, $A_2^{(1)}$, $A_3^{(1)}$ etc.

148. Teorema 3.° — *La ricerca di $B_1^{(1)}$ si riduce a quella di una sostituzione mutabile ad $A_1^{(1)}$ e che permuta gl'indici di $A_1^{(1)}$ appartenenti alle serie meno lunghe.* Sia

$$A_1^{(1)} = \begin{vmatrix} y & K_0 y \\ z & K_0(z+y) \\ u & K_0(u+z) \\ y' & K_0 y' \\ z' & K_0(z'+y') \\ u' & K_0(u'+z') \\ y'' & K_0 y'' \\ z'' & K_0(z''+y'') \end{vmatrix} \qquad B_1^{(1)} = \begin{vmatrix} y & f(y, z, u, y', z', u', y'', z'') \\ z & \varphi(y, z, u, y', z', u', y'', z'') \\ u & \psi(y, z, u, y', z', u', y'', z'') \\ y' & f'(y, z, u, y', z', u', y'', z'') \\ z' & \varphi'(y, z, u, y', z', u', y'', z'') \\ u' & \psi'(y, z, u, y', z', u', y'', z'') \\ y'' & f''(y, z, u, y', z', u', y'', z'') \\ z'' & \varphi''(y, z, u, y', z', u', y'', z'') \end{vmatrix}.$$

Per essere $A_1^{(1)}$ mutabile a $B_1^{(1)}$ è necessario che siano identiche le alterazioni che $A_1^{(1)}B_1^{(1)}$ e $B_1^{(1)}A_1^{(1)}$ fanno subire agl'indici y, z, u, perciò sarà, dividendo per K_0

$$\begin{aligned}
& f(y\,,\, z+y\,,\, u+z\,,\, y',\, z'+y',\, u'+z',\, y'',\, y''+z'') \\
= & f(y\,,\, z\,,\, u\,,\, y',\, z',\, u',\, y'',\, z'') \\
& \varphi(y\,,\, z+y\,,\, u+z\,,\, y',\, z'+y',\, u'+z',\, y'',\, y''+z'') \\
= & \varphi(y\,,\, z\,,\, u\,,\, y',\, z',\, u',\, y'',\, z'')+f(y\,,\, z\,,\, u\,,\, y',\, z',\, u',\, y'',\, z'') \\
& \psi(y\,,\, z+y\,,\, u+z\,,\, y',\, y'+z',\, u'+z',\, y'',\, y''+z'') \\
= & \psi(y\,,\, z\,,\, u\,,\, y',\, z',\, u',\, y'',\, z'')+\varphi(y\,,\, z\,,\, u\,,\, y',\, z',\, u',\, y'',\, z'').
\end{aligned}$$

Dalla 1ª relazione si deduce che f non debba contenere z, z', z'', u, u', quindi dalla 2ª si ha che φ non debba contenere u ed u', e che i coefficienti di z, z', z'' debbano essere rispettivamento uguali a quelli di y, y', y'' in f; perciò dalla 3ª si rileva che i coefficienti di u e di u' in ψ debbano essere uguali rispettivamente a quelli di z e di z' in φ, che φ non debba contenere z'', perciò f debba essere indipendente da y'', e che i coefficienti di z, z', z'' in ψ debbano essere rispettivamente uguali a quelli di y, y', y'' in φ.

Analogamente si dimostrerebbe che f' debba solo contenere y ed y'; che φ' debba essere indipendente da u, u', z'' ed i coefficienti di z e di z' debbano essere rispettivamente uguali a quelli di y e di y' in f'; che i coefficienti di u e di u' in ψ' debbano essere rispettivamente uguali a quelli di y e di y' in f e quelli di z, z', z'' a quelli di y, y', y'' in ψ'.

In forza di quanto testè è stato detto si può stabilire che $B_1^{(1)}$ debba avere la seguente forma

$$B_1^{(1)} = \left|\begin{array}{ll}
y & ay+by' \\
z & my+ny'+py''+az+bz' \\
u & ry+sy'+ty''+mz+nz'+pz''+au+bu' \\
y' & a'y+b'y' \\
z' & m'y+n'y'+p'y''+a'z+b'z' \\
u' & r'y+s'y'+t'y''+m'z+n'z'+p'z''+a'u+b'u' \\
y'' & a''y+b''y'+c''y'' \\
z'' & m''y+n''y'+p''q''+a''z+b''z'+c''z''
\end{array}\right|$$

Or se poniamo

$$C = \left|\begin{array}{ll}
y & ay+by' \\
z & my+ny'+py''+az+bz' \\
u & ry+sy'+ty''+mz+nz'+pz''+au+bu' \\
y' & a'y+b'y' \\
z' & m'y+n'y'+p'y''+a'z+b'z' \\
u' & r'y+s'y'+t'y''+m'z+n'z'+p'z''+a'u+b'u' \\
y'' & y'' \\
z'' & z''
\end{array}\right|$$

e

$$D = \begin{vmatrix} y & y \\ z & z \\ u & u \\ y' & y' \\ z' & z' \\ u' & u' \\ y'' & \beta y + \beta' y' + c'' y'' \\ z'' & \alpha y + \alpha' y' + a'' y'' + \beta z + \beta' z' + c'' z'' \end{vmatrix}$$

saranno C e D due operazioni mutabili con $A_1^{(1)}$ perchè hanno la stessa forma di $B_1^{(1)}$. La prima sarà una sostituzione se $\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}$ è diverso da zero, perchè il suo determinante è una potenza di $\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}$. La seconda equivale a due operazioni E e F delle quali l'una sostituisce a z'' e ad y'' rispettivamente $a''y'' + c''z''$, $c''y''$ e l'altra accresce quest' indici rispettivamente delle quantità

$$\alpha y + \alpha' y' + \beta z + \beta' z', \quad \beta y + \beta' y'.$$

ed ambedue sono mutabili ad $A_1^{(1)}$ per avere la stessa forma di $B_1^{(1)}$. Ma il determinante di F è 1, dunque perchè D sia una sostituzione è necessario che E abbia un determinante diverso da zero.

Ora, essendo α, α', β, β' delle costanti arbitrarie, conosciuta la sostituzione E mutabile ad $A_1^{(1)}$ lo sarà anche D; e prendendo la C sotto la forma indicata in cui le sole costanti a, b, a', b' sodisfino alla condizione che $\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}$ sia diverso da zero e moltiplicandola per D si ha una sostituzione della forma $B_1^{(1)}$; dunque la determinazione di $B_1^{(1)}$ si riduce a quella di E che non altera gl'indici y, z, u; y', z', u' delle serie più lunghe.

149. Ora ci proponiamo di trovare il numero delle sostituzioni B mutabili ad un altra A.

Supponiamo che la caratteristica di A si decomponga in tre fattori irriducibili; allora la A, ridotta alla sua forma canonica, si potrà decomporre in tre sostituzioni A_1, A_2, A_3 delle quali ciascuna è relativa alle radici di un medesimo fattore, quindi ogni sostituzione B mutabile ad A si dovrà generalmente decomporre in tre sostituzioni B_1, B_2, B_3 rispettivamente mutabili ad A_1, A_2, A_3. Or se indichiamo con K una radice del fattore corrispondente ad A_1, questa sostituzione si potrà porre sotto la forma di un prodotto di altre sostituzioni $A_1^{(1)}$, $A_1^{(2)}$ etc. l'una delle quali è relativa alla radice K, che supporremo essere $A_1^{(1)}$, e l'altre alle conjugate di K: ed analogamente B_1 si potrà scomporre in altre sostituzioni $B_1^{(1)}$, $B_1^{(2)}$ etc. rispettivamente mutabili alle precedenti, e la ricerca di B_1 dipende da quella di $B_1^{(1)}$. Similmente la determinazione di B_2 e di B_3 dipende da quella di altre sostituzioni $B_2^{(1)}$, $B_3^{(1)}$ analoghe a $B_1^{(1)}$, quindi se indichiamo con N, N', N'' i numeri delle sostituzioni $B_1^{(1)}$, $B_2^{(1)}$, $B_3^{(1)}$ sarà N N' N'' il numero delle sostituzioni B mutabili ad A.

150. Determiniamo il numero N. La sostituziono $B_1^{(1)}$ risulta dal prodotto delle altro due C o D, delle quali la seconda non altera gl'indici delle serie più lunghe. Ora se C_α o $C_{\alpha'}$ sono due sostituzioni C e D_α, $D_{\alpha'}$ due sostituzioni D, non può essere $C_\alpha D_\alpha = C_{\alpha'} C_{\alpha'}$ senza essore $C_\alpha = C_{\alpha'}$, $D_\alpha = D_{\alpha'}$; infatti le due operazioni $C_\alpha D_\alpha$, $C_{\alpha'} D_{\alpha'}$ debbono produrre gli stessi cambiamenti sopra gl'indici delle serie più lunghe, ma questi indici non sono alterati dalle sostituzioni D_α, $D_{\alpha'}$, dunque dovrà essere $C_\alpha = C_{\alpha'}$ donde $D_\alpha = D_{\alpha'}$. Adunque se indichiamo con L il numero delle sostituzioni C e con M quello delle sostituzioni D sarà $N = LM$, ma le sostituzioni D risultano da due operazioni E, F, quindi se indichiamo con P o Q i numeri delle E e delle F sarà $M = PQ$ e perciò $N = LPQ$.

151. Per determinare L osserviamo che in C entrano tante costanti quante sono quelle che si trovano nelle funzioni lineari che si scambiano con u ed u', ed in ciascuna di queste funzioni entrano tutti gl'indici corrispondenti alla radice K; per modo che se questi indici sono q di numero o si dividono in m serie di n indici, in m' di n' indici, in m'' di n'' indici etc. ciascuna delle funzioni che si scambiano con u, u' ... conterrà $mn + m'n' + m''n''$ + etc. indici, ma il numero degli u, u'... è m, dunque C conterrà $m(mn + m'n' + m''n'' + \text{etc.})$ costanti.

Di queste costanti le m^2 a, b, ...; a', b', ...; ... sono sottoposte alla condizione che il determinante

$$S = \begin{vmatrix} a, & b, & \dots \\ a', & b', & \dots \\ \dots & \dots & \dots \end{vmatrix}$$

sia diverso da zeru, e l'altro $m(mn + m'n' + \dots - m)$ possono essere scelte in p^l maniere diverse, essendo l il grado di K, quindi se indichiamo con L' il numero delle a, b, ...; a', b', ...; ... sarà

$$L = L' p^{lm(mn + m'n' + \dots - m)}.$$

152. Per determinare L' osserviamo che se si hannu p^{lm} quantità distinte col simbolo $A_{x \cdot x_1 \cdots x_{m-1}}$ nel quale ciascuno degl'indici può assumere p^l valori della forma $\alpha + \beta K + \dots + K^{l-1}$, perchè l'operazione

$$S' = [x, \; x_1 \dots \quad ax + bx_1 + \dots, \quad a'x + b'x_1 + \dots, \dots]$$

rappresentasse una vera sostituzione dovrebbe essere il determinante S diverso da zero, dunque il numero delle costanti a, b, ...; a', b', ...; ... sarà uguale a quello delle sostituzioni S', che con un ragionamento analogo a quello fatto nei n.ri (119) e (120) si trova uguale a

$$(p^{ml} - 1)(p^{ml} - p^l) \dots (p^{ml} - p^{(m-1)l}).$$

153. Infine le sostituzioni F consistono nell'accrescere ciascuno degl'ultimi indici z'' degli m' sistemi di n' indici di una funzione lineare degli n' indici di ciascuno degli m sistemi di n indici, nell'accrescere ciascuno degl'ultimi indici z''' degli m'' sistemi di n'' indici di una funzione lineare degli n'' primi indici di ciascuno degli m sistemi di n indici, e così di seguito; per modo che per effetto di queste

sole operazioni intruducono $m\,m'n' + m\,m''m' +$ etc. costanti, ciascuna delle quali può variare in p^l modi diversi. Inoltre fissati i valori di queste costanti sono determinate le funzioni che sostituiscono agl'altri indici y'' etc. quindi sarà

$$Q = p^{l(m\,m'n' + m\,m''n'' + \text{etc.})}.$$

154. Riunendo i risultati precedenti si ha l'altro

$$N = LPQ = p^{ml[m(n-1)+2(m'n'+m''n''+\dots)]}(p^{lm}-1)(p^{ml}-p^l)\dots(p^{ml}-p^{(m-1)l})\,P.$$

in cui P è ciò che diviene P se il numero degl'indici fosse $m'n' + m''n'' + \dots$ invece di $mn + m'n' + m''n'' + \dots$; per modo che si ha similmente

$$P = p^{m'l[m'(n'-1)+2(m''n''+\dots)]}(p^{m'l}-1)(p^{m'l}-p^l)\dots(p^{m'l}-p^{(m'-1)l})\,P_1$$

essendo P_1 ciò che diverrebbe N se il numero degli indici fosse $m''n'' + \dots$, e così di seguito.

CAPO 7.°

Fasci di sostituzioni tra loro mutabili.

155. Teorema 1.° – *Siano* G *un fascio di sostituzioni tra loro mutabili contenuto nel gruppo lineare di grado* p^n e $p^\pi d$, $p^{\pi'}d'$, $p^{\pi''}d''$ etc. *i gradi delle sostituzioni* S, S'_1, S_2 etc. *che lo compongono*: 1.° G *conterrà i due gruppi*

$$F = (S^{p^\pi}, S_1^{p^{\pi'}}, \dots), \qquad E = (S^d, S_1^{d'} \dots)$$

dalle cui sostituzioni si deducono tutte quelle del fascio: 2° *l'ordine di ogni sostituzione di* F *è primo con* p, *e quello di una sostituzione di* E *è una potenza di* p.

Siano $S^{\alpha p^\pi} S_1^{\beta p^{\pi'}}$, $S_2^{\alpha' p^{\pi''}} S_3^{\beta' p^{\pi'''}}$ due sostituzioni di F. È evidente che ciascuna sia mutabile con una sostituzione qualunque S_m del fascio, poichè S_m è mutabile per ipotesi con ciascuna dell'altre S, S_1, S_2, S_3. Per la stessa ragione ciascuna sostituzione di E è mutabile con ciascuna sostituzione del fascio. Quindi F ed E sono contenuti nel fascio.

Poichè p^π è primo con d, possiamo determinare due numeri interi l, m tali che si abbia

$$lp^\pi + md \equiv 1 \pmod p,$$

quindi sarà

$$S^{lp^\pi + md} = S$$

ed S risulterà dalle due sostituzioni S^{p^π}, S^d. Analogamente si dimostrerebbe che un'altra qualunque delle sostituzioni di G risulta dalle sostituzioni di E e di F.

Siano $A = S^{p^\pi} S_1^{p^{\pi'}}$, $A' = S^d S_1^{d'}$ due sostituzioni appartenenti rispettivamente ad F e ad E. Innalzando la prima alla potenza dd' e la seconda alla potenza $p^\pi p^{\pi'}$ si avrà

$$A^{dd'} = (S^{p^\pi d})^{d'} (S_1^{p^{\pi'} d'})^d = 1$$

$$A'^{p^\pi p^{\pi'}} = (S^{p^\pi d})^{p^{\pi'}} (S_1^{p^{\pi'} d'})^{p^\pi} = 1,$$

quindi dd' e $p^{\pi+\pi'}$ o saranno gl'ordini rispettivi di A e di A', ovvero dei loro mul-

tipli, dunque l'ordine di una sostituzione qualunque di F è primo con p, e quello di una sostituzione qualunque di E è una potenza di p.

156. Teorema 2.° — *Tutte le sostituzioni di F si possono ridurre alla loro forma canonica con un medesimo sistema d'indici.*

Poichè l'ordine di una sostituzione qualunque di F è primo con p, se indichiamo con a, b, c etc. le radici della congruenza caratteristica di una sostituzione A di questo gruppo, e con

$$x\,,\; x',\; x'' \ldots x^{(m-1)}\,;\quad y\ldots\,;\quad z\ldots\,;\ldots$$

le serie d'indici corrispondenti a queste radici, sarà

$$A = \left|\begin{matrix} x\,,\; x'\,,\; x'',\ldots x^{(m-1)} & ax\,,\; ax',\; ax'',\;\ldots\; ax^{(m-1)} \\ y \;\ldots\ldots & by\;\ldots\ldots \\ z\;\ldots\ldots & cz\;\ldots\ldots \\ \ldots\ldots & \ldots\ldots \end{matrix}\right|.$$

Sia A' un'altra sostituzione di F. Poichè A' è mutabile ad A, dovrà A' scambiare gl'indici che sono moltiplicati per un medesimo fattore da A con funzioni dei medesimi indici, quindi A' sarà il prodotto di più sostituzioni ciascuna delle quali fa variare gl'indici che da A sono moltiplicati per la stessa quantità.

Supponiamo che quella la quale opera sugl'indici x, x', ... $x^{(m-1)}$ sia

$$A_1 = \left|\begin{matrix} x & \alpha x + \ldots\ldots + \gamma x^{(m-1)} \\ . & \ldots\ldots \\ . & \ldots\ldots \\ . & \ldots\ldots \\ x^{(m-1)} & \alpha_{m-1}x + \ldots\ldots + \gamma_{m-1}x^{(m-1)} \end{matrix}\right|.$$

Per ridurre questa sostituzione alla sua forma canonica è necessario di risolvere la congruenza

(1) $$\left|\begin{matrix} \alpha - K & \ldots\ldots & \gamma \\ \ldots\ldots & & \\ \alpha_{m-1} & \ldots\ldots & \gamma_{m-1} - K \end{matrix}\right| \equiv 0,\; (\mathrm{mod}\, p)$$

il che è sempre possibile. Infatti A moltiplicando per a gl'indici x, x', ... $x^{(m-1)}$, se a è immaginario i coefficienti α, γ, ... α_{m-1} ... γ_{m-1} non potranno contenere altro immaginario che a, e se a è reale, lo saranno anche questi coefficienti. In questa 2ª ipotesi la precedente congruenza è a coefficienti reali, perciò ammette m radici. Nella 1ª ipotesi dovendo a essere radice della congruenza caratteristica di A, la quale è a coefficienti reali, sarà a radice di una congruenza irriducibile a coefficienti reali, la quale potrà essere o l'anzidetta o un suo fattore. Quindi se indichiamo con a, a_1, ... a_{l-1} le radici di questa congruenza irriducibile, e con $\varphi(K)$, $\varphi_1(K)$, ... $\varphi_{l-1}(K)$ il 1° membro della (1) e gl'altri che da esso si ottengono scambiando a successivamente in a_1 ... a_{l-1}, la congruenza

(2) $$\varphi(K)\,\varphi_1(K)\ldots\varphi_{l-1}(K) \equiv 0 \;(\mathrm{mod}\, p)$$

sarà a coefficienti reali, perchè il 1° membro è simmetrico per rispetto ad a.

$a_1, \ldots a_{l-1}$, per conseguenza i coefficienti delle diverse potenze di K sono esprimibili razionalmente in funzione dei coefficienti della congruenza irriducibile di cui $a, a_1 \ldots a_{l-1}$ sono le radici. Quindi la (2) ammetterà lm radici e per conseguenza l'altra

$$q(\mathrm{K}) \equiv 0 \pmod{p}$$

ne ammetterà m. Indicando con a', b', c', etc. queste radici, e con m', m'', etc. gl'ordini rispettivi di moltiplicità, la sostituzione A_1 potrà essere posta sotto la forma

$$(x_0, x_1, \ldots, x_{m-1} \quad a'x_0, \ldots, a'x_{m'-1}, \quad b'x_{m'}, \ldots, b'x_{m'+m''-1}, \ldots)$$

Operando un'analoga trasformazione sopra ciascuno dei fattori di A', si potrà ridurre questa sostituzione alla sua forma canonica.

Or se si trasforma A prendendo per indici quelli della nuova forma di A', A non perderà la sua forma canonica, poichè uno dei nuovi indici p. e. x_1 è una funzione lineare degli altri $x, x', \ldots, x^{m-1}$, ed essendo questi moltiplicati per a da A, anche x_1 sarà moltiplicato per a da A.

157. Supponiamo che F oltre delle sostituzioni che si deducono da A e da A' ne contenga dell'altre, e che A'' sia una di queste. A'' essendo mutabile ad A dovrà scambiare gl'indici $x_0, x_1, x_2, \ldots, x_{m-1}$ che A moltiplica per a con funzioni dei medesimi indici, ma A'' essendo mutabile ad A' deve scambiare gl'indici $x_0, x_1, \ldots, x_{m'-1}$ che A' moltiplica per a' con funzioni dei medesimi indici, dunque A'' deve scambiare $x_0, x_1, \ldots x_{m'-1}$ con funzioni di questi soli indici, per conseguenza può riguardarsi A'' come il prodotto di più sostituzioni ciascuna delle quali fa variare gl'indici che da A' sono moltiplicati per una stessa quantità.

Sia

$$\mathrm{A}_2 = (x_0, \ldots, x_{m'-1}, \quad \alpha_0 x_0 + \ldots + \gamma_0 x_{m'-1}, \ldots, \alpha_0^{(m'-1)} x_0 + \ldots + \gamma_0^{(m'-1)} x_{m'-1})$$

quella che fa variare gl'indici $x_1, \ldots, x_{m'-1}$. Questa sostituzione potrà essere ridotta alla sua forma canonica risolvendo la congruenza

$$(3) \qquad \begin{vmatrix} \alpha_0 - \mathrm{K} & \ldots\ldots\ldots & \alpha_0^{(m'-1)} \\ \ldots\ldots & \ldots\ldots\ldots & \ldots\ldots \\ \gamma_0 & \ldots\ldots\ldots & \gamma_0^{m'-1} - \mathrm{K} \end{vmatrix} \equiv 0 \pmod{p},$$

il che è sempre possibile. Infatti gl'indici $x_0, x_1, \ldots, x_{m'-1}$, essendo moltiplicati per a' da A', saranno funzioni di a' e degli indici $x, x', \ldots, x^{(m-1)}$, ma questi sono funzioni di a e degl'indici primitivi, dunque $x_0, x_1, \ldots, x_{m'-1}$ saranno funzioni di a, a' e degl'indici primitivi e per conseguenza se a ed a' sono immaginarii i coefficienti $\alpha_0 \ldots \gamma_0; \ldots \alpha_0^{(m'-1)} \ldots \gamma_0^{(m'-1)}$, non conterranno altri immaginari che a ed a'. Or dovendo essere a' radice di una congruenza irriducibile a coefficienti reali, se indichiamo con l' il suo grado, con $a'_2 \ldots a'_{l'-1}$ le altre sue radici, e con $\psi(\mathrm{K})$, $\psi_1(\mathrm{K}), \ldots, \psi_{l'-1}(\mathrm{K})$ il 1° membro della (3) ed i risultati che si ottengono sostituendo in esso in luogo di a successivamente $a_1 \ldots a_{l-1}$, ed in luogo di a' successivamente $a'_1 \ldots a'_{l'-1}$, la congruenza

$$\psi(\mathrm{K}), \ \psi_1(\mathrm{K}) \ldots \psi_{ll'-1}(\mathrm{K}) \equiv 0 \pmod{p}$$

sarà a coefficienti reali, per essere simmetrica per rispetto ad $a, a_1 \ldots a_{l-1}$ e per

rispetto ad $a', a'_1 \dots a'_{r-1}$, quindi ammetterà $ll'm$ radici e per conseguenza l'altra

$$\psi(K) \equiv 0 \pmod{p}$$

ne ammetterà m'. Nel caso che una delle quantità a ed a' fosse reale un ragionamento analogo al precedente ci condurrebbe alla stessa conseguenza, la quale reggerà anche quando a ed a' fossero reali, perchè allora la precedente congruenza sarebbe a coefficienti reali.

Riducendo analogamente ciascun fattore di A″ si ridurrà questa sostituzione alla sua forma canonica. E trasformando A ed A′ col sostituire agl'indici $x_0, x_1 \dots x_{m'-1} \dots$ quelli a cui si rapporta la nuova forma di A″, le due sostituzioni A ed A′ non perderanno la loro forma canonica.

Si seguiterebbe a ragionare allo stesso modo se F contenesse altre sostituzioni diverse da quelle che si deducono da A, A′, A″.

158. Risulta dal precedente ragionamento che ridotte tutte le sostituzioni di F alla loro forma canonica con un sistema d'indici, ciascuno di essi sia funzione degl'indici primitivi e delle costanti per cui è moltiplicato dalle sostituzioni elementari A, A′, etc.

159. Teorema 3.° — *Le costanti per cui uno stesso indice è moltiplicato dalle sostituzioni elementari* A, A′ etc. *sono funzioni di uno stesso immaginario.*

Poichè ogni sostituzione può essere riguardata come il prodotto di quelle delle sue potenze i di cui ordini sono potenze di numeri primi, così possiamo supporre che gl'ordini delle sostituzioni elementari A, A′ etc. siano le potenze π^μ, $\pi'^{\mu'}$ etc. dei numeri primi π, π' etc.

Consideriamo quelle delle indicate sostituzioni i di cui ordini siano potenze dello stesso numero π. Dico che le costanti $a, a', a'' \dots$ per cui esse moltiplicano lo stesso indice x siano funzioni di una di esse. Infatti se π^μ, π^{μ_1} etc. sono gl'ordini di queste sostituzioni dovrà essere

$$a^{\pi^\mu} \equiv a'^{\pi^{\mu_1}} \equiv \dots \equiv 1 \pmod{p};$$

quindi gli esponenti delle minime potenze di a, a' etc. che sono congrue ad 1 debbono essere dei divisori di π^μ, π^{μ_1} etc. Supponiamo che siano π^λ, $\pi^{\lambda'}$ etc. questi esponenti, e che λ sia il più grande dei numeri $\lambda, \lambda', \dots$, allora sarà $(a^{\pi^{\lambda-\lambda'}})^{\pi^{\lambda'}}$ la minima potenza di $a^{\pi^{\lambda-\lambda'}}$ che sia congrua ad 1, ma se $p^{l'}-1$ è la prima delle quantità $p-1$, p^2-1, $p^3-1, \dots$ che sia divisibile per $\pi^{\lambda'}$, un immaginario i la di cui minima potenza congrua ad 1 sia $i^{\pi^{\lambda'}}$ è di grado l', dunque a' ed $a^{\pi^{\lambda-\lambda'}}$ sono di grado l', ma gl'immaginarii dello stesso grado sono esprimibili in funzione razionale di uno di essi, dunque a' è funzione di $a^{\pi^{\lambda-\lambda'}}$ e quindi di a: analogamente si dimostrerebbe che a'' etc. siano funzioni razionali di a.

Ora consideriamo quelle delle sostituzioni elementari di F i di cui ordini siano le potenze π^μ, $\pi'^{\mu'}$, $\pi''^{\mu''}$ etc. di numeri primi diversi. Siano a, a_1, a_2, etc. le quan-

tità per cui esse moltiplicano lo stesso indice x. Dico che esse siano funzioni dell'immaginario $a\,a_1\,a_2 \ldots = i$ il quale sodisfa alla condizione

$$i^{\pi^{\mu}}\, i^{\pi'^{\mu'}}\, i^{\pi''^{\mu''}} \ldots \equiv 1.$$

Infatti essendo π^{μ} e $\pi'^{\mu'}\pi''^{\mu''}\ldots$ due numeri primi tra loro si possono determinare due numeri r ed r' tali che si abbia

$$r\pi'^{\mu'}\,\pi''^{\mu''}\ldots \equiv r\pi^{\mu} + 1\,.$$

ma

$$i^{r\pi'^{\mu'}\pi''^{\mu''}} \ldots \equiv a^{r\pi'^{\mu'}\pi''^{\mu''}}$$

quindi sarà

$$i^{r\pi'^{\mu'}\pi''^{\mu''}} \ldots \equiv a.$$

Analogamente si dimostrerebbe che a_1, a_2 etc. sono funzioni di i. Ma si è dimostrato che le quantità per cui quelle delle sostituzioni A, A' etc. i di cui ordini sono potenze di uno stesso numero primo moltiplicano x sono funzioni di una di esse; dunque resta dimostrato il teorema enunciato.

160. Essendo a, a', a'', etc. funzioni dell'immaginario i, gl'indici x, x', x'', etc. che da A, A', A'' etc. sono moltiplicati rispettivamente per a, a', a'', etc. saranno altresì funzioni di i, quindi se r è il grado di quest'immaginario sarà

$$x = X + i\,Y + \ldots + i^{r-1} Z\,, \quad x' = X' + i\,Y' + \ldots + i^{r-1} Z', \ldots$$

Ora se tra le altre serie d'indici a cui sono riferite A, A', A'' etc. non vi sono tutte le conjugate di x, x', x'' etc. possiamo trasformare A, A', A'' etc. in altre che sodisfano a questa condizione.

Infatti A moltiplica x, x', x'' etc. per $a = f(i)$, quindi moltiplica per $a_\rho = f(i^{p^\rho})$ i conjugati x_ρ, x'_ρ, x''_ρ, etc. corrispondenti alla radice i^{p^ρ}, per conseguenza x_ρ, x'_ρ, x''_ρ etc. debbono essere funzioni lineari degl'indici di una sola serie z_ρ, z'_ρ, z''_ρ etc. che sono moltiplicati da A, A', A'' etc. rispettivamente per a_ρ, a'_ρ, a''_ρ etc. Quest'indici sono distinti da x, x', x'' etc., perchè la sostituzione A A' A'' etc. moltiplicando x, x', x'' etc. per $a\,a'a'' \ldots = i$ moltiplicherà z_ρ, z'_ρ, z''_ρ etc. per i^{p^ρ} che è diverso da i.

Inoltre gl'indici z_ρ, z'_ρ, z''_ρ etc. sono esprimibili in funzioni lineari di x_ρ, x'_ρ, x''_ρ etc. Infatti z_ρ, z'_ρ, z''_ρ etc. sono funzioni di i^{p^ρ} per essere moltiplicati rispettivamente per a_ρ, a'_ρ, a''_ρ etc. che sono funzioni di i^{p^ρ}, perciò sarà

$$z_\rho = X_1 + i^{p^\rho} Y_1 + \ldots + i^{p^\rho(r-1)} Z_1\,, \quad z'_\rho = X'_1 + i^{p^\rho} Y'_1 + \ldots + i^{p^\rho(r-1)} Z'_1\,, \ldots,$$

e sostituendo in quest'espressioni i in luogo di i^{p^ρ}, si avranno le conjugate

$$z = X_1 + i\,Y_1 + \ldots + i^{r-1} Z_1\,, \quad z' = X'_1 + i\,Y'_1 + \ldots + i^{r-1} Z'_1\,,$$

le quali debbono essere moltiplicate da A, A', A'' etc. rispettivamente per a, a', a'' etc. quindi z, z', z'' etc. debbono essere funzioni lineari solo di x, x', x'', etc. e per conseguenza z_ρ, z'_ρ, z''_ρ etc. debbono essere funzioni lineari di x_ρ, x'_ρ, x''_ρ etc.

Ora essendo le quantità x_ρ, x'_ρ etc. funzioni lineari dell'altro z_ρ, z'_ρ etc. e viceversa, deve il numero delle prime essere uguale a quello delle seconde, altrimenti o le prime o le seconde non sarebbero tra loro indipendenti. Laonde possiamo agl'indici z_ρ, z'_ρ etc. sostituire gl'altri x_ρ, x'_ρ etc.

161. Ora se μ è il numero degl'indici x, x', etc. e dei loro conjugati si avranno le $\mu\nu$ equazioni

$$x = X + i X + ... + i^{\nu-1} Z\,, \qquad x' = X' + i\, Y' + ... + i^{\nu-1} Z', ...$$
$$x_1 = X + i^p Y + ... + i^{p(\nu-1)} Z\,, \qquad x'_1 = X' + i^p Y' + ... + i^{p(\nu-1)} Z', ...$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

dalle quali si possono ricavare i valori delle $\mu\nu$ quantità X, Y, ... le quali saranno indipendenti tra loro e potranno essere prese per indici in luogo di x, x', ... o dei loro conjugati, ed operando analogamente per le altre serie d'indici si potranno trasformare le sostituzioni di F in altre ad indici reali.

162. Teorema 3.° — *Si dividano gl'indici a cui si riferiscono le forme canoniche delle sostituzioni di F in serie riunendo quelli che sono moltiplicati per un medesimo fattore da ciascuna delle sostituzioni elementari A, A' etc. Indi si dividano le serie in sistemi riunendo quelle che sono tra loro conjugate. Infine si dividano i sistemi in classi riunendo quelli che sono formati dallo stesso numero d'indici divisi nello stesso numero di serie.*

Ogni sostituzione del gruppo I permutabile al fascio F scambierà gl'indici di una stessa serie con funzioni lineari di quelli di una medesima serie: quelli di un medesimo sistema con funzioni lineare di quelli di un medesimo sistema: quelli di una classe con funzioni lineari di quelli di questa medesima classe.

Siano $\quad A = (x, x', ... y, y', ... ax, ax', ... by, by', ...)$

una sostituzione di F, ed

$$S = \begin{vmatrix} x & \alpha x + \alpha_1 x' + ... + \beta y + \beta_1 y + \beta_1 y' + ... \\ x' & \alpha' x + \alpha'_1 x' + ... + \beta' y + \beta'_1 y + \beta'_1 y' + ... \\ \cdots & \cdots\cdots\cdots\cdots \end{vmatrix}$$

una sostituzione di I. La trasformata di A per S sarà

$$\begin{vmatrix} \alpha x + \alpha_1 x' + ... + \beta y + \beta_1 y' + ... & \alpha ax + \alpha_1 ax' + ... + \beta by + \beta_1 by' + ... \\ \alpha' x + \alpha'_1 x' + ... + \beta' y + \beta'_1 y' + ... & \alpha' ax + \alpha'_1 ax' + ... + \beta' by + \beta'_1 by' + ... \\ \cdots & \cdots \end{vmatrix},$$

ma questa trasformata deve far parte di F, quindi deve moltiplicare i primi indici per un fattore costante, per conseguenza, indicando con K questo fattore, si avrà

$$\alpha ax + \alpha_1 ax' + ... + \beta by + \beta_1 by' + ... \equiv K(\alpha x + \alpha_1 x' + ... + \beta y + \beta_1 y' + ...)$$
$$\alpha' ax + \alpha'_1 ax' + ... + \beta' by + \beta'_1 by' + ... \equiv K(\alpha' x + \alpha'_1 x' + ... + \beta' y + \beta'_1 y' + ...)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

donde $(K-b)\beta\equiv 0, \quad (K-b)\beta_1\equiv 0 \ldots (K-a)\alpha\equiv 0, \quad (K-a)\alpha_1\equiv 0 \ldots$

$(K-b)\beta'\equiv 0, \quad (K-b)\beta'_1\equiv 0 \ldots (K-a)\alpha'\equiv 0, \quad (K-a)\alpha'_1\equiv 0 \ldots$

. . . .

ma una delle quantità $\beta, \beta_1, \ldots$ deve essere diversa da zero, ed una dell'altre a, a', a'' etc. per cui le sostituzioni elementari di F moltiplicano gl'indici x, x', x'' etc. deve essere diversa da qualcuna delle quantità b, b', b'' etc. per cui le stesse sostituzioni moltiplicano y, y', y'' etc., altrimenti queste due serie d'indici ne formerebbero una sola, quindi supponendo essere

$$\beta \gtrless 0, \qquad a \gtrless b \pmod p)$$

sarà $$K\equiv b, \quad \alpha\equiv\alpha_1\equiv\ldots\equiv\alpha'\equiv\alpha'_1\equiv\ldots\equiv 0$$

ed S avrà la seguente forma

$$S=\left|\begin{array}{ll} x & \beta y+\beta_1 y'+\ldots \\ x' & \beta' y+\beta'_1 y'+\ldots \\ \ldots & \ldots\ldots \end{array}\right|.$$

Adunque ogni sostituzione di I scambierà gl'indici x, x', etc. di una stessa serie con funzioni lineari degl'indici y, y', etc. di una sola e medesima serie.

163. Ora il numero degl'indici x, x', etc. è ugualo a quello degli altri y, y', etc. Infatti le funzioni lineari di y, y' etc. che S pone in luogo di x, x', etc. debbono essere tra loro distinte, altrimenti il determinante di S sarebbe zero, ma il numero delle funzioni lineari distinte che si possono formare con y, y' etc. è al più eguale al loro numero, dunque il numero degl'indici x, x' etc. non può superare quello degl'altri y, y' cto. Inoltre S^{-1} sostituisce x, x', etc. a delle funzioni di y, y', etc., ma questa sostituziono, appartenendo ad I, non può scambiare una funzione di y, y' etc. che con una funziono degl'indici di una sola serie, adunque S^{-1} scambierà y, y' etc. con funzioni di x, x' etc. e per conseguenza il numero degl'indici y, y' etc. non può superare quello degli altri x, x', etc., ma si è detto che il numero degl'indici x, x', etc. non può superaro quello degli altri y, y' etc., adunque questi due numeri sono uguali.

164. Inoltre il numero delle serie conjugate di x, x', etc. è ugualo a quello delle serie conjugate di y, y' etc.

Infatti la trasformata di A per S moltiplica x, x', etc. per b, ma questa trasformata forma parte di F, dunque b devo essere uguale ad una delle quantità a, a', a'' etc., ma queste sono tutte funzioni di uno stesso immaginario i, dunque se ν è il grado di i vi saranno $\nu-1$ serie conjugate di x, x', etc. ed altrettanto conjugate di y, y', etc.

165. Infine ogni sostituzione di I scambia ogni serie conjugata di x, x', etc. con una serie conjugata di y, y'. etc. Infatti S, scambiando x, x', etc. con funzioni di y, y', etc., dovrà scambiare x_ρ, x'_ρ, etc. con funzioni degl'indici y_ρ, y'_ρ, etc. rispettivamente conjugati di y, y', etc.

166. Teorema 4.° – *Agl'indici pei quali le sostituzioni elementari A, A', A'', etc. di F si riducono alla loro forma canonica si possono sostituire altri indici che non alterano la loro forma, e sono così condizionali che quelli i quali appartengono ad una medesima serie si dividano in classi tali che ogni sostituzione di E non faccia che accrescere gl'indici di ciascuna classe di funzioni lineari degl'indici delle classi precedenti.*

Siano B, B', B'' etc. delle sostituzioni di E. Poichè esse debbono essere mutabili alle sostituzioni A, A'. A'' etc. di F, debbono scambiare gl'indici di un sistema con funzioni lineari degl'indici dello stesso sistema; quindi se indichiamo le mutazioni prodotte da A, A', A'' etc.; B, B', B'' etc. negl'indici del 1° sistema con A_1, A'_1, A''_1 etc.; B_1, B'_1, B''_1 etc.; in quelli del 2° con A_2, A'_2, A''_2 etc.; B_2, B'_2, B''_2 etc.: e così di seguito sarà

$$A = A_1 A_2 \ldots, \quad A' = A'_1 A'_2 \ldots, \quad A'' = A''_1 A''_2 \ldots; \ldots$$

$$B = B_1 B_2 \ldots, \quad B' = B'_1 B'_2 \ldots, \quad B'' = B''_1 B''_2 \ldots; \ldots$$

E perchè B, B', B'' etc. siano mutabili tra loro ed all'altre A, A', A'' etc. è necessario che B_1, B'_1, B''_1 etc. siano mutabili tra loro ed all'altre A_1, A'_1, A''_1 etc.; come pure che B_2, B'_2, B''_2 etc. siano mutabili tra loro ed all'altre A_2, A'_2, A''_2 etc.; e così di seguito.

Ora essendo p^π l'ordine di B, la sostituzione B^{p^π} non altera gl'indici, e quindi dovrà essere uguale ad 1 l'altra $B_1^{p^\pi}$ che indica la mutazione prodotta da B^{p^π} negli indici del 1° sistema, laonde l'ordine di B_1 sarà una potenza di p. Lo stesso è a dirsi di B'_1, B''_1, etc. e delle analoghe, quindi i gruppi

$$E_1 = (B_1, B'_1, \ldots), \quad E_2 = (B_2, B'_2, \ldots)$$

sono nelle medesime condizioni di $(B, B', B'', \ldots)$.

167. Supponiamo che gl'indici della 1ª serie del 1° sistema siano $x, x', \ldots x^{(\mu-1)}$, e che si abbia

$$B_1 = \left| \begin{matrix} x, \ldots x^{(\mu-1)}, & \alpha x + \ldots + \gamma x^{(\mu-1)}, \ldots \alpha_{\mu-1} x + \ldots + \gamma_{\mu-1} x^{(\mu-1)} \\ \ldots\ldots & \ldots\ldots\ldots\ldots \end{matrix} \right.$$

Poichè gl'indici di una serie conjugata di $x, x', \ldots x^{(\mu-1)}$ si scambiano con funzioni degl'indici della stessa serie, la congruenza caratteristica di B_1 conterrà il fattore

$$\begin{vmatrix} \alpha - K & \ldots\ldots & \alpha_{\mu-1} \\ \ldots & \ldots & \ldots \\ \gamma & \ldots\ldots & \gamma_{\mu-1} - K \end{vmatrix}$$

il quale uguagliato a zero $(\bmod p)$ darà per K dei valori che dinotano dei fattori pei quali B moltiplica delle funzioni degl'indici $x, x', \ldots x^{(\mu-1)}$. Sia μ' il numero di quelle tra queste funzioni che sono tra loro distinte.

Or poichè l'ordine di B_1 è una potenza del numero primo p, tutte le radici della sua congruenza caratteristica sono uguali ad 1, quindi saranno altresì uguali ad 1

gli anzidetti valori di K, e le μ' funzioni testè indicate non saranno alterate da B_1. Sostituiamo queste μ' funzioni agl'indici $x, x', \dots x^{(\mu'-1)}$, il che non altera la forma di A, A', A'' etc.

168. Sia B'_1 un altra sostituzione di E_1. Poichè B'_1 è mutabile con A dovrà scambiare $x, x', \dots x^{(\mu'-1)}$ con funzioni degl'indici $x, x', \dots x^{(\mu-1)}$, ma, essendo $B_1 B'_1 = B'_1 B_1$, B'_1, deve scambiare $x, x', \dots x^{(\mu'-1)}$ con funzioni d'indici che non sono alterati da B_1, quindi B'_1 deve scambiare $x, x', \dots x^{(\mu'-1)}$ con funzioni di questi stessi indici i quali non sono alterati da B_1.

Supponiamo che le funzioni colle quali B'_1 scambia gl'indici $x, x', \dots x^{(\mu'-1)}$ siano rispettivamente

$$\alpha' x + \dots + \gamma' x^{(\mu'-1)}, \quad \alpha'_1 x + \dots + \gamma'_1 x^{(\mu'-1)}, \dots, \alpha'_{\mu'-1} x + \dots + \gamma'_{\mu'-1} x^{(\mu'-1)}.$$

Allora la congruenza caratteristica di B'_1 dovrà contenere in fattore il determinante

$$\begin{vmatrix} \alpha' - K & \dots\dots & \alpha'_{\mu'-1} \\ \dots & \dots & \dots \\ \gamma' & \dots\dots & \gamma'_{\mu'-1} - K \end{vmatrix}$$

il quale uguagliato a zero $(\mathrm{mod}\, p)$ darà per K dei valori che dinotano dei fattori pei quali B'_1 moltiplica delle funzioni di $x, x', \dots x^{(\mu'-1)}$. Sia μ'' il numero di quelle tra queste funzioni che sono tra loro distinte.

Poichè l'ordine di B'_1, è una potenza di p, le radici della sua congruenza caratteristica sono uguali ad 1, perciò saranno anche uguali ad 1 gli anzidetti fattori, e le funzioni testè indicate non saranno alterate da B'_1. Prendendo queste funzioni per indici in luogo di $x, x', \dots x^{(\mu''-1)}$ le forme di A, A', A'', etc. non saranno alterate.

169. Proseguendo questo ragionamento si giungerà a conchiudere che vi sono delle funzioni di $x, x', \dots x^{(\mu-1)}$ le quali non sono alterate da alcuna delle sostituzioni di E_1. Supponendo che μ_1 sia il numero di quelle di queste funzioni che sono tra loro distinte, possiamo ammettere che esse si confondano con $x, x', \dots x^{(\mu_1-1)}$, ed allora ogni sostituzione di E_1 scambierà gl'indici $x, x', \dots x^{(\mu-1)}$ con delle funzioni delle forme seguenti

$$x, x', \dots x^{(\mu_1-1)}, \ \alpha^{(\mu_1)} x^{(\mu_1)} + \dots + \gamma^{(\mu_1)} x^{(\mu-1)} + \varphi^{(\mu_1)}, \dots \alpha^{(\mu-1)} x^{(\mu_1)} + \dots + \gamma^{(\mu-1)} x^{(\mu-1)} + \varphi^{(\mu-1)},$$

essendo $\varphi^{(\mu_1)}, \dots, \varphi^{(\mu-1)}$ delle funzioni di $x, x', \dots x^{(\mu_1-1)}$. Per modo che indicando con C_1, C'_1 etc. delle sostituzioni che cambiano $x^{(\mu_1)}, \dots x^{(\mu-1)}$ con funzioni lineari di questi stessi indici, sarà $B_1 = C_1 D_1$, $B'_1 = C'_1 D'_1$, etc.

170. Poichè D_1, D'_1 etc. accrescono di funzioni di $x, x', x^{(\mu_1-1)}$ le funzioni di $x^{(\mu_1)} \dots x^{(\mu-1)}$ che B_1, B'_1 etc. sostituiscono a questi indici, essendo B_1, B'_1 etc. tra loro mutabili, lo dovranno essere anche C_1, C'_1 etc.

Inoltre essendo $B_1^{p^\pi}$, $B_1'^{p^{\pi'}}$ etc. uguali ad 1, dovranno parimenti essere uguali ad 1 le sostituzioni $C_1^{p^\pi}$, $C_1'^{p^\pi}$ etc. quindi gl'ordini di queste sostituzioni sono delle

potenze del numero primo p, per conseguenza il gruppo $L = (C_1, C'_1, ...)$ è nelle medesime condizioni di $(B_1, B'_1, ...)$.

Di qui segue che vi saranno delle funzioni di $x^{(\mu_1)} \dots x^{(\mu-1)}$ che non saranno alterate da alcuna sostituzione di L, e che saranno accresciute di funzioni lineari di $x, x', \dots x^{(\mu_1-1)}$ dalle sostituzioni di E_1. Supponendo che μ_2 sia il numero di quelle tra queste funzioni inalterabili che siano tra loro distinte, possiamo ammettere che esse si confondano con $x^{(\mu_1)} \dots x^{(\mu_1+\mu_2-1)}$.

171. Seguitando questo ragionamento e prendendo per indici indipendenti nelle serie conjugate dell'altra $x, x', \dots x^{(\mu-1)}$ i conjugati di $x, x', \dots x^{(\mu-1)}$, si avrà per gl'indici di ciascuna serie del 1° sistema la divisione indicata nell'enunciato del teorema. Un'analoga divisione si potrà avere per quelli delle serie appartenenti ai rimanenti sistemi a cui si riferiscono i gruppi E_2 etc.

CAPO 8.°

Gruppi Primarii.

172. Un gruppo Γ contenuto nel gruppo lineare G di grado m^n dicesi *primario* quando l'altro risultante dalla combinazione delle sostituzioni di Γ con quelle del gruppo F derivato dalle sostituzioni della forma

$$(x, x', x'', \dots \quad x+\alpha, \; x'+\alpha', \; x''+\alpha'', \dots) \pmod m$$

è primitivo.

173. Affinchè G possa contenere gruppi primarii è necessario che m sia un numero primo.

Supponiamo che m contenga un fattore μ. Sia

$$A = (x, x', x'', \dots \quad ax+bx'+cx''+\dots, \quad a'x+b'x'+c'x''+\dots, \quad a''x+b''x'+c''x''+\dots, \dots)$$

una sostituzione di G. Poichè due quantità congrue secondo il modulo m lo debbono essere anche secondo il modulo μ, se si ha

$$ax+bx'+cx''+\dots\equiv\alpha, \quad a'x+b'x'+c'x''+\dots\equiv\beta, \quad a''x+b''x'+c''x''+\dots\equiv\gamma\dots \pmod m$$

dovrà anche essere

$$ax+bx'+cx''+\dots\equiv\alpha, \quad a'x+b'x'+c'x''+\dots\equiv\beta, \quad a''x+b''x'+c''x''+\dots\equiv\gamma\dots \pmod p),$$

ma se nei primi membri di queste congruenze poniamo in luogo di x, x', x'' etc. altri indici che divisi per μ danno un sistema di resti simile a quello dato da x, x', x'' etc., i secondi membri risulteranno congrui rispettivamente ad α, β, γ etc. secondo il modulo μ; quindi ogni lettera i cui indici divisi per μ danno un sistema di resti uguale a quello dato da x, x', x'' etc. sarà scambiata da A in un altra i cui indici danno per rispetto a μ un sistema di resti analogo a quello dato da da α, β, γ etc. Per conseguenza dividendo le lettere in sistemi col riunire quelle i cui indici danno per rispetto a μ un medesimo sistema di resti, ogni sostituzione di G scambierà le lettere di un sistema con quelle di un altro; e siccome lo stesso

succederà per le sostituzioni di F, anche le sostituzioni che risultano dalle combinazioni di quelle di Γ e F, si comporteranno nello stesso modo, e per conseguenza il gruppo da esse formato non sarà primitivo.

174. Teorema. *La condizione necessaria e sufficiente perchè* Γ *sia primario è che non si possa determinare un numero di funzioni indipendenti* y, y', y'' etc. *degli indici, inferiore a quello degl'indici, le quali per ogni sostituzione di* Γ *siano scambiate con funzioni delle sole* y . y', y'' etc.

Questa condizione è necessaria; poichè essendo y, y', y'' etc. tra loro indipendenti possiamo prendere queste funzioni in luogo di altrettanti indici, ed allora ogni sostituzione di Γ sarà della forma

$$(y, y', y'', \dots x^{(n-1)} \quad ay+by'+cy''+\dots \quad a'y+b'y'+c'y''+\dots \quad a^{(n-1)}y+b^{(n-1)}y+\dots+cx^{(n-1)})$$

ed ogni sostituzione di F della forma

$$(y, y', y'', \dots x^{(n-1)} \quad y+\alpha,\ y'+\beta,\ y''+\gamma, \dots x^{(n-1)}+\lambda),$$

e quindi, dividendo le lettere in sistemi col riunire quelle in cui y, y', y'' etc. hanno gli stessi valori, ogni sostituzione di Γ e di F e quindi ogni sostituzione risultante dalla combinazione di questi due gruppi scambierà le lettere di un sistema con quelle di un altro sistema, e per conseguenza Γ non sarà primario.

Inoltre questa condizione è sufficiente. Supponiamo che il gruppo risultante dalla combinazione delle sostituzioni di F e di Γ non sia primitivo e che $x_0, x'_0, x''_0, \dots$; $x_0+\alpha_0$, $x'_0+\beta_0$, $x''_0+\gamma, \dots$ siano gl'indici di due lettere appartenenti ad un medesimo sistema. È evidente che F contenga la sostituzione

$$S_0 = (x, x', x'', \dots \quad x+\alpha_0,\ x'+\beta_0,\ x''+\gamma_0, \dots)$$

la quale scambia la prima lettera nella seconda. Siano x_1, x'_1, x''_1, gl'indici di una lettera appartenente ad un altro sistema; saranno $x_1+\alpha_0$, $x'_1+\beta_0$, $x''_1+\gamma_0, \dots$ quelli della lettera in cui essa è scambiata da S_0. Ora F contiene la sostituzione

$$S' = (x, x', x'', \dots \quad x+x_0-x_1,\ x'+x'_0-x'_1,\ x''+x''_0-x''_1, \dots)$$

la quale scambia le lettere distinte dagl'indici $x_1, x'_1, x''_1, \dots$; $x_1+\alpha_0$, $x'_1+\beta_0$, $x''_1+\gamma_0, \dots$ rispettivamente con quelle che hanno per indici $x_0, x'_0, x''_0, \dots$; $x_0+\alpha_0$, $x'_0+\beta_0$, $x''_0+\gamma_0, \dots$, ma quest'ultime appartengono ad un medesimo sistema, dunque anche le prime apparterranno ad uno stesso sistema, e per conseguenza la sostituzione S_0 non sposterà i sistemi.

Scambiamo gl'indici x, x', x'', etc. negli altri

$$y = \frac{1}{\alpha_0}x, \quad y' = x' - \frac{\beta_0}{\alpha_0}x, \quad y'' = x'' - \frac{\gamma_0}{\alpha_0}x, \dots;$$

allora S_0 prenderà la seguente forma

$$S_0 = (y, y', y'', \dots \quad y+1,\ y',\ y'', \dots)$$

ad ogni sostituzione di F l'altra

$$(y, y', y'', \ldots \quad y+\beta_0, \; y'+\beta'_0, \; y''+\beta''_0, \ldots).$$

Or supponiamo che oltre la sostituzione 1 e le potenze di S_0, sia in F contenuta un'altra sostituzione che non sposti i sistemi, la quale sia

$$S' = (y, y', y'', \ldots \quad y+\beta_0, \; y'+\beta'_0, \; y''+\beta''_0, \ldots).$$

È evidente che la sostituzione

$$S' S_0^{-\beta_0} = (y, y', y'', \ldots \quad y, y'+\beta'_0, \; y''+\beta''_0, \ldots)$$

non sposti i sistemi e sia diversa da 1, quindi una almeno delle quantità β'_0, β''_0 etc. deve essere diversa da zero. Supponiamo che lo sia β'_0 e scambiamo gl'indici y, y', y'', etc. negli altri

$$z = y, \quad z' = \frac{1}{\beta'_0} y', \quad z'' = y'' - \frac{\beta''}{\beta'_0} y', \ldots,$$

allora la precedente sostituzione, che indicheremo con S_1, prenderà la seguente forma

$$S_1 = (z, z', z'', \ldots \quad z, \; z'+1, \; z'', \ldots),$$

S_0 conserverà la forma primitiva

$$S_0 = (z, z', z'', \ldots \quad z+1, \; z', \; z'', \ldots),$$

ed ogni sostituzione di F che non sposta i sistemi sarà contenuta nella espressione $S_0^a S_1^b$.

Se F contenesse un'altra sostituzione S'' che non spostasse i sistemi e non fosse compresa tra quelle espresse da $S_1^a S_1^b$, combinando S_0, S_1 ed S'' si avrebbe un'altra sostituzione S_2 diversa da 1 la quale non sposterebbe i sistemi e non altererebbe z, e z', e si potrebbe scegliere un sistema d'indici tali che S_0, S_1 ed S_2 avessero le forme seguenti

$$\begin{aligned} S_0 &= (u, u', u'', \ldots \quad u+1, \quad u', \quad u'', \ldots) \\ S_1 &= (u, u', u'', \ldots \quad u, \quad u'+1, \quad u'', \ldots) \\ S_2 &= (u, u', u'', \ldots \quad u, \quad u', \quad u''+1, \ldots). \end{aligned}$$

Procederemo in questa guisa sino a che non siano esaurite tutte le sostituzioni di F le quali non spostano i sistemi, il che dovrà succedere prima di esaurirsi le sostituzioni del gruppo F; poichè essendo questo gruppo transitivo vi saranno delle sostituzioni che sposteranno i sistemi.

Supponiamo che tutte le sostituzioni di F che non spostano i sistemi siano della forma $S_0^a S_1^b$. Se Σ è una sostituzione di F le trasformate di S_0 e di S_1 per Σ non debbono spostare i sistemi, perchè Σ scambiando le lettere di un sistema con quelle di un altro sistema l'indicate trasformate permutano tra loro le lettere dei sistemi nei quali sono mutati da Σ quelli su cui operavano S_0 ed S_1. Ma queste trasformate appartengono ad F, dunque dovrà aversi

$$\Sigma^{-1} S_0 \Sigma = S_0^a S_1^b, \qquad \Sigma^{-1} S_1 \Sigma = S_0^{a'} S_1^{b'}$$

donde

$$S_0 \Sigma = \Sigma S_0^a S_1^b, \qquad S_1 \Sigma = \Sigma S_0^{a'} S_1^{b'}. \qquad (1)$$

Or se supponiamo che fosse

$$\Sigma=(z,\ z',\ z'',\ \dots\ \ az+bz'+cz''+\dots,\ \ a'z+b'z'+c'z''+\dots,\ \ a''z+b''z'+c''z''+\dots)$$

sarebbe

$$S_0\Sigma=(z,\ z',\ z'',\dots\ \ a(z+1)+bz'+cz''+\dots,\ \ a'(z+1)+b'z'+c'z''+\dots,\ \ a''(z+1)+b''z'+c''z''+\dots)$$

$$\Sigma S_0{}^a S_1{}^b=(z,\ z',\ z'',\dots\ \ az+bz'+cz''+a,\ \ a'z+b'z'+c'z''+b,\ \ a''z+b''z'+c''z''+\dots,\dots)$$

ma queste due sostituzioni debbono essere identiche, dunque dovrà essere $a''=0$. Analogamente, mediante la seconda delle (1), si dimostrerebbe essere $b''=0$, quindi la funzione che Σ pone in luogo di z'' è indipendente da z e da z'. Analogamente si dimostrerebbe che lo stesso succede per le funzioni che Σ pone in luogo degli indici che seguono z''. Ma z'', z''' etc. sono delle funzioni degl'indici primitivi x, x', x'' etc., adunque quante volte il gruppo risultante dalla combinazione delle sostituzioni di Γ e di F non è primitivo si possono sempre determinare delle funzioni degl'indici, in numero minore di quest'indici, le quali da ogni sostituzione di Γ siano scambiate con delle espressioni, formate dalle stesse funzioni. Quindi la condizione indicata nell'enunciato è sufficiente.

CAPO 9.°

Gruppo Ortogonale.

175. Una sostituzione lineare

$$S=(x,\ y,\ z,\ \dots,\ \ ax+by+cz+\dots,\ \ a'x+b'y+c'z+\dots,\ \ a''x+b''y+c''z+\dots,\dots)$$

dicesi ortogonale se si ha

$$x^2+y^2+z^2+\dots\equiv(ax+by+cz+\dots)^2+(a'x+b'y+c'z+\dots)^2+(a''x+b''y+c''z+\dots)^2+\dots\ (\text{mod } p)$$

donde si ha

$$\begin{gathered}a^2+a'^2+a''^2+\dots\equiv b^2+b'^2+b''^2+\dots\equiv c^2+c'^2+c''^2+\dots\equiv 1\\ ab+a'b'+a''b''+\dots\equiv ac+a'c'+a''c''+\dots\equiv bc+b'c'+b''c''+\dots\equiv 0.\end{gathered}\qquad(1)$$

176. Le sostituzioni ortogonali formano un gruppo, poichè alterando ciascuna di esse di un multiplo di p la funzione $x^2+y^2+z^2+\dots$, il prodotto di due qualunque di queste sostituzioni produrrà la stessa alterazione nell'indicata funzione.

177. La reciproca di S è appunto

$$S_1=(x,\ y,\ z,\ \dots\ \ ax+a'y+a''z+\dots,\ \ bx+b'y+b''z+\dots,\ \ cx+c'y+c''z+\dots,\dots),$$

perchè in forza delle (1) il prodotto SS_1 si riduce ad 1. Ora i determinanti di S e di S_1 sono uguali, ma il loro prodotto deve essere uguale ad 1, dunque *il determinante di una sostituzione ortogonale è uguale a* ± 1.

178. Teorema 1.° – *Se s'indica con* R_n *il numero dei sistemi di sostituzioni della congruenza*

$$x_1{}^2+x_2{}^2+\dots+x_n{}^2\equiv 1\ (\text{mod } p)$$

l'ordine Ω_n *del gruppo ortogonale di grado* p^n *sarà*

$$\Omega_n=R_n\,R_{n-1}\dots R_1.$$

Indichiamo con T_0, T_1 ... le sostituzioni del gruppo ortogonale che non spostano l'indice x, e con S una sostituzione del medesimo gruppo che pone $ax+by+cz+...$ in luogo di x. Allora le sole sostituzioni ST_0, ST_1, ... produrranno lo stesso cambiamento. Invero se U è una sostituzione che scambia x in $ax+by+cz+...$, l'altra $S^{-1}U$, lasciando l'indice x invariato, apparterrà alla serie $T_0, T_1, \dots$, e quindi $SS^{-1}U=U$ farà parte dell'altra serie ST_0, ST_1 etc. Ma se nelle relazioni che stabiliscono l'ortogonalità della sostituzione

$$S=(x, y, z, \dots, \quad ax+by+cz+\dots, \quad a'x+b'y+c'z+\dots, \quad a''x+b''y+c''z+\dots, \dots)$$

poniamo $a\equiv 1$, $b\equiv c\equiv \dots \equiv 0$, si hanno appunto le relazioni che stabiliscono l'ortogonalità della sostituzione

$$T=(x, y, z, \dots \quad x, \quad a'x+b'y+c'z+\dots, \quad a''x+b''y+c''z+\dots, \dots),$$

quindi le sostituzioni T_0, T_1, etc. formano il gruppo ortogonale di grado p^{n-1}; per conseguenza se indichiamo con Q_n il numero delle funzioni $ax+by+cz+...$ che le sostituzioni del gruppo proposto pongono in luogo di x, sarà

$$\Omega_n = Q_n \Omega_{n-1} = Q_n Q_{n-1} \Omega_{n-2} = \dots = Q_n Q_{n-1} Q_{n-2} \dots \Omega_1,$$

ma Ω_1 è evidentemente uguale al numero delle soluzioni della congruenza

$$x^2 \equiv 1 \pmod p,$$

dunque sarà dimostrato il teorema proposto qualora lo sarà l'uguaglianza

$$Q_n = R_n;$$

ma la S non può essere una sostituzione ortogonale se non esiste la relazione

$$a^2+b^2+c^2 \dots \equiv 1 \pmod p, \tag{1}$$

dunque sarà evidente la precedente uguaglianza quando avremo dimostrato che ad ogni soluzione a, b, c etc. della (1) corrisponde una sostituzione S del gruppo ortogonale.

179. Primo caso. $n=2$. Se a, b è una soluzione della congruenza

$$x_1^2+x_2^2 \equiv 1 \pmod p$$

vi sarà la sostituzione ortogonale

$$S=(x, y, \quad ax+by, \quad -bx+ay)$$

la quale scambia x in $ax+by$,

180. Secondo caso. $n=3$. Sia a, b, c una soluzione della congruenza

$$x_1^2+x_2^2+x_3^2 \equiv 1 \pmod p, \tag{2}$$

e supponiamo che $1-b^2$ sia un residuo quadratico congruo a t^2; allora sarà

$$\frac{b^2}{t^2}+\frac{c^2}{t^2} \equiv \frac{1-b^2}{t^2} \equiv 1$$

e la sostituzione $S_1=\left(x, y, z \quad x, \quad \frac{a}{t}y+\frac{c}{t}z, \quad \frac{-c}{t}y+\frac{a}{t}z\right)$

sarà ortogonale; ma anche le seguenti

$$S_2=(x, y, z \quad y, x, z), \qquad S_3=(x, y, z \quad bx+ty, \quad -tx+by, \quad z)$$

sono ortogonali, dunque lo sarà anche $S_2 S_1 S_3$, ma questa sostituzione pone $ax+by+cz$ in luogo di x, adunque alla soluzione a, b, c della (2) corrisponde una sostituzione S.

181. Or supponiamo che nessuna delle tre differenze $1-a^2$, $1-b^2$, $1-c^2$ sia un residuo quadratico. Allora possiamo fare due ipotesi.

Prima ipotesi $\left(\frac{-1}{p}\right)=+1$. Se esiste la sostituzione ortogonale

$$S'=(x,\ y,\ z\quad ax+b'y+c'z,\ldots)$$

nella quale si ha $\quad b'\equiv b\beta-c\gamma,\quad c'\equiv c\beta+b\gamma,\quad \beta^2+\gamma^2\equiv 1$

vi sarà anche l'altra $\quad S=(x,\ y,\ z\quad ax+by+cz,\ldots)$.

Invero la sostituzione $S''=(x, y, z\quad x,\quad \beta y+\gamma z,\quad -\gamma y+\beta z)$

è ortogonale, quindi lo sarà anche $S''^{-1}S'$, ma

$$S''^{-1}=(x,\ y,\ z\quad x,\quad \beta y-\gamma z,\quad \gamma y+\beta z),$$

dunque $S''^{-1}S'$ scambierà x in $ax+by+cz$, e sarà $S''^{-1}S'=S$.

Analogamente si dimostrerebbe che esistendo la sostituzione

$$S'''=(x,\ y,\ z\quad a'x+b'y+c''z,\ldots)$$

nella quale fosse $\quad a'\equiv a\alpha-c'\delta,\quad c''\equiv a\delta+c'\alpha,\quad \alpha^2+\delta^2\equiv 1$

esisterebbe anche S' e quindi S.

Or b' deve acquistare almeno $\frac{p+1}{2}$ valori diversi col variare di α e di β. Invero se immaginiamo che b' avesse un valore determinato, eliminando β tra le due congruenze

$$b'\equiv b\beta-c\gamma,\quad \beta^2+\gamma^2\equiv 1$$

si avrebbe una congruenza di 2° grado in γ la quale non ammetterebbe che due radici, perciò non vi sono che due sistemi di valori per β o γ che possono dare lo stesso valore di b', ma $p+1$ è il numero delle soluzioni della congruenza

$$\beta^2+\gamma^2\equiv 1\ (\mathrm{mod}\, p),$$

dunque b' deve avere almeno $\frac{p+1}{2}$ valori diversi.

Tra questi valori ve ne deve essere almeno uno pel quale $1-b'^2$ o è un residuo ovvero è congruo a zero. Infatti i valori di b'^2 pei quali $1-b'^2$ è non residuo renderanno b'^2-1 un residuo, essendo -1 non residuo, ma b'^2 è anche residuo, dunque i valori di b'^2 che renderanno $1-b'^2$ non residuo saranno tanti quanti sono i residui seguiti da residui nella serie $1, 2, 3\ldots p-1$, ma questi sono $\frac{p-3}{4}$ (107), dunque questo sarà il numero dei valori di b'^2 pei quali $1-b'^2$ è non residuo; ma a ciascun valore di b'^2 corrispondono due valori di b', adunque vi sono $\frac{p-3}{2}$ valori di b' pei quali $1-b'^2$ è non residuo, ma il numero dei valori distinti di b' è $\frac{p+1}{2}$, dunque vi dovrà essere un valore di b' per cui $1-b'^2$ o è congruo a zero ovvero è un residuo.

Analogamente si dimostrerebbe che tra i valori che assumo a' col variare di α e di δ ve ne debba essere almeno uno per cui $1-a'^2$ o è un residuo ovvero è congruo a zero.

Da quanto si è detto risulta che possono darsi i due casi: 1° che sia $1-b'^2 \equiv 0$, $1-a'^2 \equiv 0$: 2° che sia una delle differenze $1-a'^2$, $1-b'^2$ un residuo quadratico. Ma il 1° caso non può aver luogo, perchè essendo

$$a'^2+b'^2+c''^2 \equiv a^2+b'^2+c'^2 \equiv a^2+b^2+c^2 \equiv 1\,,$$

sarebbe $c''^2 \equiv -1$ e quindi -1 sarebbe residuo, il che è contrario all'ipotesi fatta, dunque dovrà aver luogo il 2° caso ed in conseguenza esisterà la S.

182. *Seconda ipotesi* $\left(\frac{-1}{p}\right)=1$. Essendo -1 residuo quadratico, se $1-b'^2$ è non residuo lo sarà altresì b'^2-1. Ora per essere b'^2-1 non residuo è necessario che b'^2 rappresenti uno dei residui della serie $1, 2, 3, \ldots p-1$ che sono preceduti da non residui, ma il numero di questi residui è $\frac{p-1}{4}$, dunque vi saranno $\frac{p-1}{4}$ valori di b'^2 pei quali $1-b'^2$ è non residuo, ma a ciascun valore di b'^2 corrispondono due valori di b', dunque vi saranno $\frac{p-1}{2}$ valori di b' pei quali $1-b'^2$ sarà non residuo. Ma nell'ipotesi fatta, essendo $p-1$ il numero delle soluzioni della congruenza

$$\beta^2+\gamma^2 \equiv 1 \pmod{p},$$

il numero dei valori distinti di b' è almeno $\frac{p-1}{2}$, dunque, variando β e γ, b' o assumerà tutt'i valori d per cui $1-b'^2$ è non residuo ovvero prenderà qualche valore per cui $1-b'^2$ è residuo, ovvero qualche valore per cui $1-b'^2$ è congruo a zero.

Analogamente si dimostrerebbe che, variando α e δ, a' o assumerà tutt'i valori per cui $1-a'^2$ è non residuo, o prenderà qualche valore per cui $1-a'^2$ è residuo, ovvero qualche valore per cui $1-a'^2$ è congruo a zero.

183. Combinando l'ipotesi che si possono fare sopra i valori di $1-b'^2$ con quelle che si possono fare sopra i valori di $1-a'^2$, e tralasciando quella in cui si suppone che una delle differenze $1-a'^2$, $1-b'^2$ è residuo per cui è dimostrata l'esistenza di S, possiamo distinguere i seguenti casi.

1° Caso. $1-b'^2 \equiv 0$, $1-a'^2 \equiv 0$. Esisterà la S''' e quindi la S se esiste la sostituzione ortogonale

$$S^{\text{IV}} = (x, y, z \quad a''x+b''y+c''z, \ldots)$$

essendo $\quad a'' \equiv a'\varepsilon - b'\zeta, \quad b'' \equiv a'\zeta + b'\varepsilon, \quad \varepsilon^2+\zeta^2 \equiv 1.$

Or se indichiamo con λ un numero tale che sia $\lambda^2 \equiv -1$, le soluzioni della congruenza

$$\varepsilon^2+\zeta^2 \equiv 1 \pmod{p}$$

saranno date (106) dalle altre tre

$$\varepsilon-\lambda\zeta \equiv v\,, \quad \varepsilon+\lambda\zeta \equiv u\,, \quad uv \equiv 1 \pmod{p}$$

e quindi saranno date dalle formole

$$\varepsilon \equiv \frac{1}{2}\left(v + \frac{1}{v}\right), \qquad \zeta \equiv \frac{1}{2\lambda}\left(v - \frac{1}{v}\right),$$

essendo v un intero arbitrario, ma si ha

$$1 - a''^2 \equiv 2\, a'b'\varepsilon\zeta,$$

dunque sarà
$$1 - a''^2 \equiv \frac{a^2b^2}{2\lambda}\left(v^2 - \frac{1}{v^2}\right) = \frac{a^2b^2}{2\lambda v^2}(v^4 - 1),$$

e perciò $1 - a''^2$ sarà un residuo quadratico se $\frac{a^2b^2}{2\lambda}$ o $v^4 - 1$ sono simultaneamente residui o non residui; ma secondo Gauss si può determinare v in modo che $v^4 - 1$ sia residuo o non residuo, dunque $1 - a''^2$ è un residuo e per conseguenza ha luogo la sostituzione ortogonale S^{iv}.

184. 2° Caso. $a' \equiv \pm 1$, $b' \equiv \pm d$. Nella serie $1, 2 \ldots p - 1$ vi è un residuo p' preceduto da un non residuo $p' - 1$ e seguito da un residuo $p' + 1$. Infatti se 2 è residuo lo sarà anche $p - 2$, e se $p - 3$ è non residuo sarà $p - 2 = p'$. Ma se $p - 3$ fosse residuo, procedendo da $p - 3$ verso 1 nella serie $1, 2 \ldots p - 1$ s'incontrerebbe necessariamente un residuo p' seguito da un residuo $p' + 1$ e preceduto da un non residuo $p' - 1$. Che se 2 non è residuo, tra i residui maggiori di 2 ve ne dovrà anche essere uno condizionato come quello indicato da p': infatti se così non fosse ciascuno dei $\frac{p-1}{2} - 2$ residui maggiori di 2 e minori di $p - 1$ dovrebbe essere compreso tra due non residui, e quindi la serie

$$\left(\frac{1}{p}\right),\ \left(\frac{2}{p}\right), \ldots\ldots \left(\frac{p-1}{p}\right)$$

presenterebbe $p - 3$ variazioni, mentre effettivamente ne presenta $\frac{p-1}{2}$; invero, essendovi $\frac{p-1}{4}$ residui seguiti da non residui nella serie $1, 2 \ldots p - 1$, nella serie precedente vi saranno $\frac{p-1}{4}$ passaggi dal + al −, ma i due termini estremi sono positivi per modo che il numero dei passaggi dal + al − è uguale a quello dei passaggi dal − al +, dunque il numero delle variazioni della suindicata serie è $\frac{p-1}{2}$.

Ora possiamo fare $d^2 \equiv p'$, perchè sarebbe $d^2 - 1 \equiv p' - 1$ e quindi $d^2 - 1$ ed $1 - d^2$ sarebbero non residui; ma allora essendo

$$1 - c''^2 \equiv a'^2 + b'^2 \equiv 1 + p'$$

sarebbe $1 - c''^2$ un residuo come lo è $1 + p'$, dunque nel caso in parola esisterà S''' e quindi S.

185. 3° Caso. $a' \equiv d$, $b' \equiv d'$ essendo d e d' due numeri scelti arbitrariamente nella serie di quelli per cui $1 - a'^2$ ed $1 - b'^2$ sono non residui.

Si ha
$$d^2 + d'^2 + c''^2 \equiv a'^2 + b'^2 + c''^2 \equiv a^2 + b^2 + c^2 \equiv 1$$

quindi per ogni sistema di valori di d e di d' vi sono due valori di d'' che sodisfano alla relazione

$$d^2 + d'^2 + d''^2 \equiv 1$$

che sarebbero $\pm c''$, ma abbiamo innanzi veduto che d e d' possono avere $\frac{p-1}{2}$ valori diversi, quindi combinando in tutt' i modi possibili i valori di d e di d' si avranno $\frac{1}{2}(p-1)^2$ soluzioni della precedente congruenza. Ora esisterà la sostituzione S se vi sarà l'altra ortogonale

$$S^{(1)} = (x, y, z \quad dx + d'y + c''z, \ldots),$$

la quale avrà luogo se vi sarà l'altra

$$S^{(2)} = (x, y, z \quad dx + d'y - c''z, \ldots),$$

poichè ponendo $\qquad T = (x, y, z \quad x, y, -z)$

la sostituzione $TS^{(2)}$ pone $dx + d'y + c''z$ in luogo di x. Quindi perchè nel caso in parola non esistesse la S sarebbe necessario che non avesse luogo questa sostituzione per tutte le soluzioni a, b, c della congruenza (1) per cui $1 - a^2$ ed $1 - b^2$ sono non residui. Or questo è impossibile. Infatti la S esiste per tutte l'altre soluzioni della (1) che sono in numero di $p^2 + p - \frac{1}{2}(p-1)^2$, perciò sarà

$$R_3 = p^2 + p - \frac{1}{2}(p-1)^2 = \frac{1}{2}(p^2 + 4p - 1),$$

ma è $\Omega_2 = 2(p-1)$, dunque sarà

$$\Omega_3 = R_3\,\Omega_2 = (p^2 + 4p - 1)(p-1).$$

Ma il gruppo ortogonale di grado p^3 è contenuto nel gruppo lineare dello stesso grado il di cui ordine è

$$\Omega'_3 = (p^3 - 1)(p^3 - p)(p^3 - p^2),$$

dunque dovrà essere Ω'_3 divisibile per Ω_3, ma $p^2 + 4p - 1$ è primo con p, dunque dovrà essere $(p^3 - 1)(p^2 - 1)$ divisibile per $p^2 + 4p - 1$, il che non è: infatti se $p^2 + 4p - 1$ dividesse

$$(p^3 - 1)(p^2 - 1) \equiv -4p\,(p^3 - 1)$$

dividerebbe $\qquad 4(p^3 - 1) \equiv 68p - 20,$

ma essendo -1 residuo di p sarà

$$p \equiv 1 \pmod 4$$

donde $\qquad 68p - 20 \equiv 0 \pmod{16}$

$$p^2 + 4p - 1 \equiv 4 \pmod 8,$$

dunque il quoto sarebbe $\equiv 0 \pmod 4$, e perciò $p^2 + 4p - 1$ dividerebbe $17p - 5$; il che è impossibile, perchè, se p è maggiore di 12, il valore di $p^2 + 4p - 1$ è maggiore di quello di $17p - 5$, e se p è minore di 12 deve essere p uguale a 5 che è il solo numero primo minore di 12 che abbia la forma $1 + 4n$, e per questo valore di p il numero $17p - 5$ non è divisibile per l'altro $p^2 + 4p - 1$.

186. Terzo caso $n > 3$. Con ragionamenti analoghi a quelli fatti innanzi si vedrebbe che esiste una sostituzione ortogonale che pone $ax + by + cz + dv + \dots$ in luogo di x se, essendo a, b, c, d etc. una soluzione della congruenza

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + \dots \equiv 1 \pmod p$$

o una delle differenze $1 - a^2$, $1 - b^2$ etc. è un residuo quadratico, ovvero due delle quantità a, b, c, etc. sono congrue a ± 1.

Supponiamo che non si verifichi alcuno di questi due casi. Allora tra le quantità a^2, b^2, c^2, etc. ve ne debbono essere tre la di cui somma è diversa da zero, poichè se fosse altrimenti o tutte le quantità a, b, c, etc. sarebbero congrue a ± 1, ovvero una o più delle differenze $1 - a^2$, $1 - b^2$, $1 - c^2$, etc. sarebbero residui quadratici. Infatti se n è della forma $3k + 1$, dovendo essere la somma degli n quadrati a^2, b^2 etc. congrua ad 1 e quella di $n - 1$ qualunque di essi congrua a zero, sarà il rimanente congruo ad 1, e quindi tutte le quantità a, b, c etc. saranno congrue a ± 1: che se n è della forma $3k + 2$ sarà la somma di due qualunque di questi quadrati congrua ad 1 e quindi la somma di sei quadrati congrua a 3, ma questa somma deve essere anche congrua a zero, dunque dovrà essere $p = 3$ e quindi uno qualunque di questi quadrati o è congruo ad 1 ovvero a zero, e se è congruo a zero la differenza che si ottiene togliendolo da 1 sarà residuo quadratico.

187. Supponiamo che sia $a^2 + b^2 + c^2 \equiv m \gtrless 0$. Sia

$$S = (x, y, z, u, \dots \quad \alpha x + \beta y + \gamma z, \quad \alpha' x + \beta' y + \gamma' z, \quad \alpha'' x + \beta'' y + \gamma'' z, \quad u, \dots)$$

una sostituzione ortogonale. È evidente che se, essendo

$$a'\alpha + b\beta + c\gamma \equiv a', \quad a\alpha' + b\beta' + c\gamma' \equiv b', \quad a\alpha'' + b\beta'' + c\gamma'' \equiv c',$$

esiste una sostituzione ortogonale della forma

$$S_1 = (x, y, z, u, \dots \quad a'x + b'y + c'z + du + \dots, \dots)$$

esisterà anche una sostituzione ortogonale che porrà $ax + by + cz + du + \dots\dots$ in luogn di x, la quale sarà SS_1.

Ora possiamo determinare i valori di α, β, γ in modo da rendere uno dei tre coefficienti a', b', c', p. e. a' congruo a zero, cosicchè $1 - a'^2$ sarà un residuo quadratico e la S_1 sarà possibile.

Infatti, essendo $a^2 + b^2 + c^2 \gtrless 0$, non possono essere tutti e tre i quadrati a^2, b^2, c^2 congrui a zero. Supponiamo che sia $a^2 \gtrless 0$: allora uguagliando a zero il valore di b' e ricavando il valore di α si avrà $\alpha = -\frac{b\beta + c\gamma}{a}$, e sostituendo questo valore nella congruenza

$$\alpha^2 + \beta^2 + \gamma^2 \equiv 1$$

si otterrà $\quad b^2\beta^2 + c^2\gamma^2 + 2bc\beta\gamma + a^2\beta^2 + a^2\gamma^2 \equiv a^2$

ovvero $\quad (a^2 + b^2)\beta^2 + 2bc\beta\gamma + (a^2 + c^2)\gamma^2 \equiv a^2, \qquad (2)$

Se le due quantità $a^2 + b^2$, $a^2 + c^2$ sono congrue a zero questa congruenza si ridurrà all' altra

$$2bc\beta\gamma \equiv a^2$$

la quale può essere soddisfatta da valori determinati di β e di γ, perchè b e c debbono essere diversi da zero altrimenti lo sarebbe anche a, il che è contrario all' ipotesi.

Ma se $a^2 + b^2$ ed $a^2 + c^2$ sono diversi da zero, poniamo

$$(a^2 + b^2)\beta + bc\gamma = \beta',$$

cosicchè la (2) prenderà la seguente forma

$$\beta'^2 + (a^2 + b^2)\{(a^2 + c^2) - b^2c^2\}\gamma^2 \equiv a^2(a^2 + b^2),$$

e siccome il coefficiente di γ^2 si riduce ad ma^2 che è diverso da zero, così la (2) ammetterà $p - \left(\frac{-ma^2}{p}\right)$ soluzioni. Trovati i valori di β' e di γ si avranno per mezzo di essi quelli di β e di α.

CAPO 10.°

Gruppo Abeliano.

188. Indichiamo con I il gruppo derivato dalle sostituzioni

$$A_1 = (z_1\, z_2 \ldots\, z_1 + 1,\, z_2 \ldots), \qquad A_2 = (z_1\, z_2 \ldots\, z_1\, z_2 + 1), \ldots \pmod p$$

essendo p un numero primo, e siano

$$S = A_1^{m_1} A_2^{m_2} A_3^{m_3} \ldots, \qquad S_1 = A_1^{n_1} A_2^{n_2} A_3^{n_3} \ldots$$

due sostituzioni di I. Poichè S ed S_1 sono tra loro mutabili possiamo sostituire S_1S ad SS_1. Per conservare in questo mutamento la traccia della sostituzione SS_1 donde è stata dedotta l' altra S_1S procediamo nel seguente modo.

Dinotiamo con $(A_\mu A_\nu)$ il passaggio da $A_\mu A_\nu$ ad $A_\nu A_\mu$, allora quello da SS_1 ad S_1S sarà espresso da

$$m_1n_1(A_1A_1) + m_1n_2(A_1A_2) + \ldots + m_2n_1(A_2A_1) + \ldots \tag{1}$$

Diamo ad (A_1A_2), $(A_1A_3) \ldots (A_2A_1) \ldots, \ldots$ dei valori arbitrarii scambiabili con altri ad essi congrui secondo il modulo p, avendo riguardo alle due relazioni

$$(A_\mu A_\mu) \equiv 0, \quad (A_\mu A_\nu) + (A_\nu A_\mu) \equiv 0 \pmod p$$

risultanti dai due fatti: 1° che la sostituzione $A_\mu A_\mu$ non perde la sua forma se il secondo A_μ si scrive prima dell' altro: 2° che la sostituzione $A_\mu A_\nu$ si riproduce nella medesima sua forma se prima si scambia A_μ con A_ν, ed indi nella forma risultante $A_\nu A_\mu$ si scambia A_ν con A_μ.

In tal modo la (1) avrà un valore numerico che possiamo scambiare con qualunque altro ad esso congruo secondo il modulo p, e sostituendo

$$1^{m_1n_1(A_1A_1)+m_1n_2(A_1A_2)+\ldots}\, S_1\, S \tag{2}$$

ad $S\,S_1$ si conserverà la traccia di $S\,S_1$ donde è stata dedotta $S_1\,S$. All'esponente che ha 1 nella (2) si dà il nome di *esponente di mutamento* delle due sostituzioni S ed S_1.

189. *Possiamo scegliere in I tante sostituzioni quanti sono gl' indici $z_1\, z_2$ etc., le quali siano così condizionate che l' esponente di mutamento di ciascuna per rispetto ad una qualunque delle rimanenti sia o 1 ovvero zero.*

Supponiamo che si possano dare tali valori ad $(A_1 A_2)$ $(A_1 A_3)$ etc. che resti sodisfatta la condizione

$$\begin{vmatrix} (A_1 A_1) & (A_1 A_2) & \dots \\ (A_2 A_1) & (A_2 A_2) & \dots \\ \dots & \dots & \dots \end{vmatrix} \gtrless 0 \qquad (3).$$

Allora in I vi sarà la sola sostituzione 1 il di cui esponente di mutamento con tutte l'altre sia zero. Infatti se ve ne fosse un'altra $A_1^m A_2^n A_3^p \dots$ che soddisfacesse a questa condizione dovrebbero reggere le congruenze

$$m\,(A_1 A_1) + n\,(A_1 A_2) + \dots \equiv 0$$
$$m\,(A_2 A_1) + n\,(A_2 A_2) + \dots \equiv 0 \pmod p$$
$$\dots\dots\dots\dots\dots\dots$$

il che è impossibile posta la (3).

Ciò premesso siano S_1 ed S' due sostituzioni di I il di cui esponente di mutamento sia congruo a $\lambda \pmod p$ ed ε un numero tale che si abbia

$$\lambda \varepsilon \equiv 1 \pmod p.$$

Evidentemente si avrà

$$(S_1\, S'^{\varepsilon}) \equiv 1 \pmod p.$$

Dinotiamo con S'' un'altra sostituzione di I i di cui esponenti di mutamento con S_1 ed $S'^{\varepsilon} = T_1$ siano rispettivamente b e $-a$, sarà

$$S'' = S_1^a\, T_1^b\, U$$

essendo U una sostituzione del gruppo I' le cui sostituzioni hanno zero per esponente di mutamento con S_1 e T_1.

Siano S_2 ed S''' due sostituzioni di I' per le quali si abbia $(S_2\, S''') \equiv \lambda'$. Determinando un numero ε' tale che fosse

$$\lambda' \varepsilon' \equiv 1 \pmod p,$$

sarà

$$(S_2\, S'''^{\varepsilon'}) \equiv 1,$$

ed ogni sostituzione di I' potrà mettersi sotto la forma $S_2\, T_2\, U'$ indicando con U' una sostituzione del gruppo I'' le di cui sostituzioni hanno zero per esponente di mutamento con S_2 e T_2, e con T_2 la sostituzione $S'''^{\varepsilon'}$.

Continuando in questo modo si giungerà al gruppo formato dalla sola sostituzione 1; laonde ogni sostituzione di I si potrà porre sotto la forma

$$S_1^a\, T_1^b\, S_2^c\, T_2^d \qquad (4)$$

essendo S_1, T_1, S_2, T_2 etc. delle sostituzioni tali che si abbia pei valori 1, 2, 3 etc. di μ e di ν

$$\left.\begin{aligned} (S_\mu\, T_\mu) \equiv -(T_\mu\, S_\mu) \equiv 1 \\ (S_\mu\, T_\nu) \equiv (T_\nu\, S_\mu) \equiv (S_\mu\, S_\nu) \equiv (S_\nu\, S_\mu) \equiv (T_\mu\, T_\nu) \equiv (T_\nu\, T_\mu) \equiv 0. \end{aligned}\right\} \pmod p$$

Inoltre il numero delle sostituzioni S_1, T_1, S_2, T_2 etc. è uguale a quello delle

altre A_1, A_2, A_3 etc. e quindi uguale al numero degl' indici z_1, z_2, z_3 etc. Infatti potendosi ogni sostituzione di I porre sotto la forma (4), ovvero sotto l'altra

$$A_1^{\alpha} A_2^{\beta} A_2^{\gamma} A_3^{\delta} \qquad (5)$$

è necessario che il numero dei sistemi di valori di a, b, c, d etc. sia uguale a quello dei sistemi di valori di $\alpha, \beta, \gamma, \delta$ etc., il che non può succedere se il numero delle sostituzioni A_1, A_2 etc. non sia uguale a quello dell'altre C_1, T_1 etc.

190. Or siccome il numero delle sostituzioni S_1, T_1 etc. è pari, così sarà anche pari il numero delle sostituzioni A_1, A_2 etc., ma queste sono tante quanti sono gl' indici, dunque nel caso che si considera il numero degl' indici è pari.

191. *Si possono scambiare gl' indici* z_1, z_2 etc. *in altri*

$$u_1 = az_1 + bz_2 + \ldots, \qquad u_2 = a'z_1 + b'z_2 + \ldots, \ldots$$

tali che le sostituzioni S_1, T_1, S_2, T_2 etc. *accrescano di* 1 *rispettivamente gl' indici* u_1, u_2, u_3, u_4 etc. *senza alterare gl' altri.*

Infatti supponiamo che sia

$$S_1 = A_1^{\alpha} A_2^{\beta} \ldots, \qquad T_1 = A_1^{\alpha'} A_2^{\beta'} \ldots, \ldots$$

sarà

$$S_1^x T_1^y \ldots = A_1^{\alpha x + \alpha' y + \ldots} A_2^{\beta x + \beta' y + \ldots} \ldots,$$

e siccome ogni sostituzione di I può mettersi sotto una delle forme (4) e (5) così è necessario che si potessero determinare per $x_1\ y_1$ etc. dei valori tali che le quantità

$$\alpha x + \alpha' y + \ldots, \qquad \beta x + \beta' y + \ldots, \ldots$$

risultassero congrue a dei numeri dati; quindi è necessario che fosse

$$\begin{vmatrix} \alpha & \alpha' \ldots\ldots \\ \beta & \beta' \ldots\ldots \\ \ldots\ldots\ldots\ldots \end{vmatrix} \gtrless 0 \pmod{p} \qquad (6).$$

Ora le S_1, T_1 etc. mutano u_1 rispettivamente in

$$u_1 + a\alpha + b\beta + \ldots, \qquad u_1 + a\alpha' + b\beta' + \ldots, \ldots$$

u_2 rispettivamente in

$$u_2 + a'\alpha + b'\beta + \ldots, \qquad u_2 + a'\alpha' + b'\beta' + \ldots, \ldots$$

e così di seguito: ma avendo luogo la (6) si potranno determinare $a, b, \ldots\ldots; a', b', \ldots; \ldots$ in modo che siano sodisfatte le condizioni

$$\begin{array}{ll} a\alpha + b\beta + \ldots \equiv 1 & a'\alpha + b'\beta + \ldots \equiv 0 \ldots \\ a\alpha' + b\beta' + \ldots \equiv 0 & a'\alpha' + b'\beta' + \ldots \equiv 1 \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots & \end{array}$$

quindi S_1, T_1 etc. accresceranno di un'unità rispettivamente u_1, u_2 etc. senza alterare gl' altri indici.

192. È evidente che la trasformata di una sostituzione qualunque di I per mezzo di una sostituzione lineare appartenga allo stesso gruppo I. Ciò premesso stabiliamo il seguente:

Teorema I.° — *Tutte le sostituzioni del gruppo lineare G di grado p^{2n} che trasformano due sostituzioni qualunque di I in altre il di cui esponente di mutamento sia congruo a quello delle due che si trasformano moltiplicato per una costante formano un gruppo.*

Siano R ed S due sostituzioni di I, T e T' due sostituzioni di G, R' ed S' le trasformate di R e di S per T, ed R'_1, S'_1 le trasformate di R' e di S'' per T'. Inoltre supponiamo che si abbia

$$(R' S') \equiv m\,(RS), \quad (R'_1\, S'_1) \equiv m'\,(R' S').$$

Essendo $$(TT')^{-1}\, RTT' = T'^{-1}\, T^{-1}\, RTT' = T'^{-1}\, R'\, T' = R'_1$$

$$(TT')^{-1}\, STT' = T'^{-1}\, T^{-1}\, STT' = T'^{-1}\, S'\, T' = S'_1$$

saranno R'_1, S'_1 rispettivamente le trasformate di R e di S per TT', ma si ha

$$(R'_1\, S'_1) \equiv m'\,(R' S') \equiv mm'\,(R\, S)$$

dunque l'esponente di mutamento delle trasformate di R e di S per TT' è congruo al prodotto di una costante mm' per l'esponente di mutamento (RS), dunque le sostituzioni T, T' e l'analoghe formeranno un gruppo.

Il gruppo formato dalle sostituzioni T dicesi *gruppo Abelliano.*

193. Affinchè una sostituzione lineare possa appartenere al gruppo di Abel è sufficiente che essa sodisfi alla condizione enunciata nel precedente teorema per rispetto alle sostituzioni elementari A_1, A_2 etc. del gruppo I.

Infatti supponiamo che essendo A'_μ ed A'_ν le trasformate di A_μ e di A_ν per la sostituzione lineare

$$T = (z_1\,,\ z_2\,,\dots \quad q'z_1 + r'z_2 + \dots\,,\quad q''z_1 + r''z_2 + \dots\,,\dots)$$

si abbia per tutt'i valori di μ e di ν la relazione

$$(A'_\mu\, A'_\nu) \equiv m\,(A_\mu\, A_\nu).$$

Inoltre siano $$R = A_1^{p_1}\, A_2^{p_2} \dots\,, \qquad S = A_1^{q_1}\, A_2^{q_2} \dots$$

due sostituzioni di I, ed

$$R' = A'^{p_1}_1\, A'^{p_2}_2 \dots\,, \qquad S' = A'^{q_1}_1\, A'^{q_2}_2 \dots$$

le loro trasformate per T.

Ora si ha $$(R' S') \equiv \Sigma p_\mu\, q_\nu\, (A'_\mu\, A'_\nu)\,,$$

e sostituendo in luogo di $(A'_\mu\, A'_\nu)$ il suo valore si ha

$$(R'S') \equiv m\, \Sigma\, p_\mu\, q_\nu\, (A_\mu\, A_\nu)$$

ma $$(R\, S) \equiv \Sigma\, p_\mu\, q_\nu\, (A_\mu\, A_\nu)$$

dunque sarà $$(R' S') \equiv m\,(R\, S)\,,$$

epperò T apparterrà al gruppo di Abel.

194. Immaginiamo che si scambino gl'indici z_1, z_2, z_3, z_4 etc. in altri $x_1, y_1, x_2, y_2, \dots$ tali che le sostituzioni elementari di I ad essi rispettivamente corrispondenti

$$S_1\,, T_1\,;\quad S_2\,, T_2\,; \qquad (7)$$

sodisfino alle condizioni

$$(S_\mu\, T_\mu) \equiv -(T_\mu\, S_\mu) \equiv 1\,,\quad (S_\mu\, S_\nu) \equiv 0\,,\quad (T_\mu\, T_\nu) \equiv 0\,,\quad (S_\mu\, T_\nu) \equiv 0$$

intendendo cho μ e ν prendano tutt'i valori da 1 a $2n$, numero degl'indici z_1. Allora supponendo che la sostituzione T riferita a questi nuovi indici prenda la forma

$$\mathrm{T} = \left| \begin{matrix} x_1, y_1 & a'_1 x_1 + c'_1 y_1 + \ldots + a'_n x_n + c'_n y_n\,, & b'_1 x_1 + d'_1 y_1 + \ldots + b'_n x_n + d'_n y_n \\ \cdots & \cdots & \cdots \\ x_n, y_n & a_1^{(n)} x_1 + c_1^{(n)} y_1 + \ldots + a_n^{(n)} x_n + c_n^{(n)} y_n\,, & b_1^{(n)} x_1 + d_1^{(n)} y_1 + \ldots + b_n^{(n)} x_n + d_n^{(n)} y_n \end{matrix} \right|$$

le sostituzioni (7) saranno dalla T trasformate nell'altre

$$\mathrm{S}'_1 = \mathrm{S}_1^{a'_1}\, \mathrm{T}_1^{b'_1}\, \mathrm{S}_2^{a_1''}\, \mathrm{T}_2^{b_1''} \ldots, \qquad \mathrm{T}'_1 = \mathrm{S}_1^{c'_1}\, \mathrm{T}_1^{d'_1}\, \mathrm{S}_2^{c_1''}\, \mathrm{T}_2^{d_1''}, \ldots$$

ed esprimendo che hanno luogo le relazioni

$$(\mathrm{S}'_\mu \mathrm{T}'_\mu) \equiv m\,(\mathrm{S}_\mu \mathrm{T}_\mu) \equiv m\,, \qquad (\mathrm{S}'_\mu \mathrm{S}'_\nu) \equiv m\,(\mathrm{S}_\mu \mathrm{S}_\nu) \equiv 0$$
$$(\mathrm{T}'_\mu \mathrm{T}'_\nu) \equiv m\,(\mathrm{T}_\mu \mathrm{T}_\nu) \equiv 0\,, \qquad (\mathrm{S}'_\mu \mathrm{T}'_\nu) \equiv m\,(\mathrm{S}_\mu \mathrm{T}_\nu) \equiv 0$$

si avrà

$$\begin{aligned} &\sum_\mu a_\nu^{(\mu)} d_\nu^{(\mu)} - b_\nu^{(\mu)} c_\nu^{(\mu)} \equiv m\,, \qquad \sum_\mu a_\nu^{(\mu)} d_{\nu'}^{(\mu)} - b_\nu^{(\mu)} c_{\nu'}^{(\mu)} \equiv 0 \quad \text{se } \nu' \gtrless \nu \\ &\sum_\mu a_\nu^{(\mu)} b_{\nu'}^{(\mu)} - b_\nu^{(\mu)} a_{\nu'}^{(\mu)} \equiv 0\,, \qquad \sum_\mu c_\nu^{(\mu)} d_{\nu'}^{(\mu)} - d_\nu^{(\mu)} c_{\nu'}^{(\mu)} \equiv 0 \pmod{p}. \end{aligned} \tag{8}$$

195. Se si operasse la sostituzione T sopra ciascuna delle due serie d'indici

$$x_1 y_1\,, x_2 y_2\,, \ldots, x_n y_n$$
$$\varepsilon_1 \eta_1\,, \varepsilon_2 \eta_2\,, \ldots, \varepsilon_n \eta_n$$

contenuti nella funzione

$$\varphi = x_1 \eta_1 - y_1 \varepsilon_1 + x_2 \eta_2 - y_2 \varepsilon_2 + \ldots + x_n \eta_n - y_n \varepsilon_n$$

essa resterebbe moltiplicata per m, sopprimendo i multipli di p, nel solo caso che avessero luogo le (8), quindi il gruppo di Abel si può definire per quello le di cui sostituzioni, operate sopra ciascuna delle due serie d'indici contenuti in φ, moltiplicano questa funzione per una costante.

196. Teorema 2.° – *L'ordine del gruppo Abelliano* G' *di grado* p^{2n} *è*

$$\Omega = (p^{2n} - 1)\, p^{2n-1} (p^{2n-2} - 1)\, p^{2n-3} \ldots (p^2 - 1)\, p\, (p - 1).$$

Indichiamo con r una radice primitiva della congruenza

$$r^{p-1} \equiv 1 \pmod{p}.$$

È evidente che la sostituzione

$$\mathrm{S} = (x_1, y_1, x_2, y_2, \ldots\;\; r x_1, y_1, r x_2, y_2, \ldots)$$

appartenga a G', poichè moltiplica φ per r; ma r può essere congrua secondo il modulo p ad una quantità qualunque, dunque ogni sostituzione di G' può essere posta sotto la forma SU, indicando con U una sostituzione di G' che non altera φ. Ma r non può avere che $p - 1$ valori incongrui tra loro secondo il modulo p, adunque se indichiamo con Ω' l'ordine del gruppo H formato dalle sostituzioni U, sarà

$$\Omega = (p - 1)\, \Omega'.$$

197. Per determinare il valore di Ω' procediamo nel seguente modo. Supponiamo che una sostituzione U di H ponga $f = a'_1 x_1 + c'_1 y_1 + \dots$ in luogo di x_1, allora ogni sostituzione di H che scambia x_1 con f potrà mettersi sotto la forma $U\Sigma$ (178), indicando con Σ una sostituzione di H che non altera x_1; quindi Ω' sarà uguale al numero delle funzioni f, ammissibili dal gruppo H, moltiplicato per l'ordine del gruppo H_1 formato dalle sostituzioni Σ; ma sono ammissibili nella composizione di f tutt'i sistemi dei valori di a_1, c_1 etc. che si ottengono facendo variare ciascuno di questi coefficienti da 0 a $p-1$, eccetto quello in cui tutti siano zero; adunque Ω' sarà uguale a $p^{2n}-1$ moltiplicato per l'ordine di H_1. Sia U' una sostituzione di H_1 che scambia y_1 in $f' = b' x_1 + d' y_1 + \dots$ Ogni sostituzione di H_1 che scambia y_1 in f' potrà porsi sotto la forma $U'\Sigma'$, indicando con Σ' una sostituzione di H_1 che non altera y_1, quindi l'ordine di H_1 sarà uguale al prodotto del numero delle f' per l'ordine del gruppo H_2 formato dalle sostituzioni Σ'; ma se nelle (8) poniamo

$$m \equiv 1\,, \quad a'_1 \equiv 1\,, \quad c'_1 \equiv a'_2 \equiv \dots \equiv 0$$

si ha $d' \equiv 1$, quindi per la composizione di f' possiamo prendere tutt'i sistemi dei valori di b'_1, d'_2 etc. che si ottengono facendo variare questi coefficienti da 0 a $p-1$, epperò l'ordine di H_1 sarà uguale al prodotto di p^{2n-1} per l'ordine Ω'' di H_2, ossia sarà

$$\Omega' = (p^{2n}-1)\, p^{2n-1}\, \Omega''$$

198. Ora H_2 è il gruppo Abelliano di grado p^{2n-2}. Infatti il moltiplicare φ per m equivale ad operare la sostituzione T sopra ciascuna delle due serie d'indici contenuti in questa funzione; quindi si avrà lo stesso risultato o se dopo aver moltiplicato φ per m si opera sugl'indici x_1, y_1 etc. la sostituzione T^{-1}, ovvero se si opera la sostituzione T sopra le due variabili ε, η; adunque se poniamo

$$T^{-1} = \begin{vmatrix} x_1, y_1 & \alpha'_1 x_1 + \gamma'_1 y_1 + \dots + \alpha'_n x_n + \gamma'_n y_n, & \beta'_1 x_1 + \delta'_1 y_1 + \dots + \beta'_n x_n + \delta'_n y_n \\ \dots & \dots & \dots \\ x_n, y_n & \alpha_1^{(n)} x_1 + \gamma_1^{(n)} y_1 + \dots + \alpha_n^{(n)} x_n + \gamma_n^{(n)} y_n, & \beta_1^{(n)} x_1 + \delta_1^{(n)} y_1 + \dots + \beta_n^{(n)} x_n + \delta_n^{(n)} y_n \end{vmatrix}$$

dovrà essere

$$m \sum_{\mu,\nu} (\alpha_\mu^{(\nu)} x_\mu + \gamma_\mu^{(\nu)} y_\mu)\eta_\nu - (\beta_\mu^{(\nu)} x_\mu + \delta_\mu^{(\nu)} y_\mu)\varepsilon_\nu \equiv \sum_{\mu,\nu} (b_\nu^{(\mu)} \varepsilon_\nu + d_\nu^{(\mu)} \eta_\nu) x_\mu - (a_\nu^{(\mu)} \varepsilon_\nu + c_\nu^{(\mu)} \eta_\nu) y_\mu$$

donde si deducono le relazioni

$$\alpha_\mu^{(\nu)} \equiv \frac{1}{m} d_\nu^{(\mu)}, \quad \gamma_\mu^{(\nu)} \equiv -\frac{1}{m} c_\nu^{(\mu)}, \quad \beta_\mu^{(\nu)} \equiv -\frac{1}{m} b_\nu^{(\mu)}, \quad \delta_\mu^{(\nu)} \equiv \frac{1}{m} a_\nu^{(\mu)}. \tag{9}$$

Or se in T fosse

$$a'_1 \equiv 1\,, \quad a'_2 \equiv \dots \equiv a'_n \equiv 0\,, \quad c'_1 \equiv c'_2 \equiv \dots \equiv 0$$
$$d'_1 \equiv 1\,, \quad d'_2 \equiv \dots \equiv d'_n \equiv 0\,, \quad b'_1 \equiv b'_2 \equiv \dots \equiv 0$$

in T^{-1} sarebbe $\quad \alpha'_1 \equiv 1 , \quad \alpha'_2 \equiv \ldots \equiv \alpha'_n \equiv 0 \quad \gamma'_1 \equiv \ldots \gamma'_n \equiv 0$

$$\beta'_1 \equiv \ldots\ldots \beta'_n \equiv 0 \quad \delta'_1 \equiv 1 \quad \delta'_2 \equiv \ldots \equiv \delta'_n \equiv 0 ,$$

quindi per le (9) sarebbe

$$a_1^{(2)} \equiv \ldots a_1^{(n)} \equiv 0 , \quad b_1^{(2)} \equiv \ldots b_1^{(n)} \equiv 0 , \quad c_1^{(2)} \equiv \ldots c_1^{(n)} \equiv 0 , \quad d_1^{(2)} \equiv \ldots d_1^{(n)} \equiv 0$$

e gli altri coefficienti di T sarebbero legati dalle relazioni esistenti tra i coefficienti degl' indici di una sostituzione appartenente al gruppo Abelliano di grado p^{2n-2}, adunque una sostituzione del gruppo Abelliano G' del grado p^{2n} che non altera una coppia d' indici appartiene al gruppo Abelliano di grado p^{2n-2}, ma H_2 contiene tutte le sostituzioni di H che non alterano x_1 ed y_1, dunque H_2 sarà un gruppo Abelliano di grado p^{2n-2}. Per conseguenza se indichiamo con Ω''' l'ordine del gruppo Abelliano di grado p^{2n-2} sarà

$$\Omega'' = (p^{2n-2} - 1)\, p^{2n-3}\, \Omega''',$$

e se Ω^{iv} indica l'ordine del gruppo Abelliano di grado p^{2n-4} sarà

$$\Omega''' = (p^{2n-4} - 1)\, p^{2n-5}\, \Omega^{iv},$$

e così di seguito, per modo che si avrà

$$\Omega' = (p^{2n} - 1)\, p^{2n-1}\, (p^{2n-2} - 1)\, p^{2n-3} \ldots (p^2 - 1)\, p$$

e quindi $\quad \Omega = (p^{2n} - 1)\, p^{2n-1}\, (p^{2n-2} - 1)\, p^{2n-3} \ldots (p^2 - 1)\, p\, (p - 1)$

199. Teorema 3.° – *Ogni sostituzione del gruppo* H *è derivata dall' altre tre*

$$M_\mu = (\ldots x_\mu , y_\mu \ldots \quad \ldots y_\mu \quad , -x_\mu \ldots)$$
$$L_\mu = (\ldots x_\mu , y_\mu \ldots \quad \ldots x_\mu + y_\mu , \quad y_\mu \ldots)$$
$$N_{\mu\cdot\nu} = (\ldots x_\mu , y_\mu \ldots x_\nu , y_\nu \ldots \quad \ldots x_\mu + y_\nu , y_\mu \ldots x_\nu + y_\mu , y_\nu \ldots).$$

Poniamo

$$L'_\mu = (\ldots x_\mu , y_\mu \ldots\ldots \quad \ldots x_\mu \quad , y_\mu + x_\mu \ldots\ldots) = M_\mu L_\mu M_\mu^{-1}$$
$$Q_{\mu\cdot\nu} = (\ldots x_\mu , y_\mu \ldots x_\nu , y_\nu \ldots \quad \ldots x_\mu + x_\nu , \ y_\mu \ldots\ldots x_\nu , \ y_\nu - y_\mu \ldots) = M_\nu^{-1} N_{\mu\cdot\nu} M_\nu$$
$$R_{\mu\cdot\nu} = (\ldots x_\mu , y_\mu \ldots x_\nu , y_\nu \ldots \quad \ldots x_\mu \quad , y_\mu - x_\nu \ldots x_\nu , \ y_\nu - x_\mu \ldots) = M_\nu^{-1} Q_{\nu\,\mu} M_\nu ,$$

Supponiamo che una sostituzione U di H scambia x_1 con $f = a'_1 x_1 + c'_1 y_1 + a'_2 x_2 + c'_2 y_2 + \ldots$, e che sia $a'_1 \gtrless 0$; allora la sostituzione

$$U_1 = L_1^{\beta} M_1 L_1^{\alpha} Q_{1\cdot 2}^{a'_2} N_{1\cdot 2}^{c'_2} \ldots Q_{1\cdot n}^{a'_n} N_{1\cdot n}^{c'_n}$$

la quale è derivata da L_μ, M_μ, $N_{\mu\cdot\nu}$ porrà f in luogo di x_1 se α e β sono determinate dalle seguenti congruenze

$$\alpha \equiv - a'_1 + a'_2 c'_2 + \ldots + a'_n c'_n , \qquad 1 + a'_1 \beta \equiv b'_1 \pmod p.$$

Che se $a'_1 \equiv 0$ ed $a''_1 \gtrless 0 \pmod p$, indicando con u una sostituzione derivata da L_μ, M_μ, $N_{\mu\cdot\nu}$ la quale scambi x_1 con $-a'_2 x_1 + b'_1 y_1 + (b'_1 + b'_2)\, y_2 + a'_3 x_3 + \ldots$, l'altra $Q_{2\cdot 1}\, u$ porrà f in luogo di x_1.

Infine se fosse $a'_1 \equiv a'_2 \equiv \ldots \equiv a'_n \equiv 0$, ma il coefficiente che ha un indice y in f, p. es. $c'_2 \gtrless 0 \pmod p$, componendo con L_μ, M_μ, $N_{\mu\cdot\nu}$ una sostituzione u' la quale scambiasse x' con $c'_2 x_2 + c'_3 y_3 + \ldots$, l'altra $M_2\, u'$ porrà f in luogo di x_1.

Quindi ogni sostituzione di H può mettersi sotto la forma $S\Sigma$, indicando con S una sostituzione derivata da L_μ, M_μ, $N_{\mu\cdot\nu}$ e con Σ una sostituzione di H la quale non alteri x_1.

Or supponiamo che Σ ponga $f' = b'_1 x_1 + d'_1 y_1 + b'_2 x_2 + d'_2 y_2 + \ldots$ in luogo di y_1. Per ciò che innanzi si è detto dovrà essere $d' \equiv 1$, quindi la sostituzione

$$S' = L'^{\,\alpha}_1\, R_{1\cdot 2}^{-b'_2}\, Q_{2\cdot 1}^{-d'_2} \ldots\ldots R_{1\cdot n}^{-b'_n}\, Q_{n\cdot 1}^{-d'_n}$$

porrà f' in luogo di y' senza alterare x', se α è determinata dalla congruenza

$$\alpha \equiv b'_1 + b'_2 d'_2 + \ldots + b'_n d'_n \pmod p;$$

laonde Σ sarà della forma $S'\Sigma'$, essendo S' una sostituzione derivata da L_μ, M_μ, $N_{\mu\cdot\nu}$ e Σ' una sostituzione di H che non fa variare x_1 ed y_1 Ora Σ' appartiene al gruppo Abelliano di grado p^{2n-2} analogo ad H, quindi essa potrà porsi sotto la forma $S''\Sigma''$ in cui S'' dinota una sostituzione derivata da L_μ, M_μ, $N_{\mu\cdot\nu}$, (essendo μ e $\nu > 1$) e Σ'' una sostituzione che non altera le due coppie d'indici x_1, y_1, y_2, y_2. Continuando in questo modo si perverrà ad una sostituzione Σ_n che non altererà alcun indice e quindi si ridurrà ad 1.

CAPO 11.°

Gruppi Ipo-abelliani.

200. Dicesi *caratteristica* della sostituzione $A_1^{m_1} A_2^{m_2} \ldots$ del gruppo I derivato dalle sostituzioni

$$A_1 = (z_1, z_2 \ldots z_1 + 1, z_2 \ldots), \qquad A_2 (z_1, z_2 \ldots z_1, z_2 + 1 \ldots) \ldots \pmod 2$$

l'espressione
$$\sum_{\mu=1}^{\mu=2n} \sum_{\nu=\mu}^{\nu=2n} (A_\mu A_\nu)\, m_\mu m_\nu + \sum_{\mu=1}^{\mu=2n} s_\mu m_\mu \pmod 2$$

nella quale s_μ dinota una quantità arbitraria che varia col variare di μ e $2n$ il numero degl' indici z_1, z_2 etc.

201. Teorema 1.° — *Il carattere di un prodotto è congruo* (mod 2) *alla somma dei caratteri dei fattori e dei loro esponenti di mutamento.*

Siano
$$S = A_1^{m_1} A_2^{m_2} \ldots, \qquad S_1 = A_1^{n_1} A_2^{n_2} \ldots$$

due sostituzioni di I. Moltiplicandole si avrà l'altra

$$SS_1 = A_1^{m_1+n_1} A_2^{m_2+n_2} \ldots$$

il di cui carattere è

$$\sum_{\mu=1}^{\mu=2n} \sum_{\nu=\mu}^{\nu=2n} (A_\mu A_\nu)(m_\mu + n_\mu)(m_\nu + n_\nu) + \sum_{\mu=1}^{\mu=2n} s_\mu (m_\mu + n_\mu)$$

$$\equiv \text{caratt. } S + \text{caratt. } S' + \sum_{\mu=1}^{\mu=2n} \sum_{\nu=\mu}^{\nu=2n} (A_\mu A_\nu)(m_\mu n_\nu + m_\nu n_\mu);$$

ma essendo $(A_\mu A_\mu) \equiv 0, \quad (A_\mu A_\nu) \equiv -(A_\nu A_\mu) = (A_\nu A_\mu) \pmod 2$

si ha $$\sum_{\mu=1}^{\mu=2n} \sum_{\nu=\mu}^{\nu=2n} (A_\mu A_\nu)(m_\mu n_\nu + m_\nu n_\mu) \equiv \sum_{\mu=1}^{\mu=2n} \sum_{\nu=1}^{\nu=2n} (A_\mu A_\nu) m_\mu n_\nu = (SS_1),$$

dunque sarà $\quad$ caratt. $SS_1 \equiv$ caratt. $S +$ caratt. $S' + (SS_1) \pmod 2$.

202. Teorema 2.° — *Le sostituzioni lineari che trasformano una sostituzione qualunque* S *di* I *in altre che hanno il medesimo carattere di* S *formano un gruppo il quale è contenuto in quello di Abel.*

Infatti siano T e T' due di queste sostituzioni lineari, S' ed S'_1 le trasformate di S per T e per T'. La trasformata di S per TT' è

$$(TT')^{-1}\, S\, TT' = T'^{-1}\, T^{-1}\, S\, TT' = T'^{-1}\, S'\, T' = S'_1$$

ma S' ha lo stesso carattere di S, ed S'_1 ha lo stesso carattere di S', dunque S'_1 avrà lo stesso carattere di S, quindi le sostituzioni T, T' e l'analoghe formeranno un gruppo.

Ora indicando con S'' la trasformata per T di un'altra sostituzione S_1 di I, si ha

caratt. $S' \equiv$ caratt. S, $\quad$ caratt. $S'' \equiv$ caratt. S_1, $\quad$ caratt. $S' S'' \equiv$ caratt. SS_1,

ma $\quad$ caratt. $S'S'' \equiv$ caratt. $S' +$ caratt. $S'' + (S'S'') \pmod 2$

caratt. $S S_1 \equiv$ caratt. $S +$ caratt. $S_1 + (S S_1) \pmod 2$,

dunque sarà $\quad (S' S'') \equiv (SS_1)$

e per conseguenza il gruppo formato dalle sostituzioni T è contenuto in quello di Abel.

203. Per esprimere le condizioni a cui deve sodisfare una sostituzione lineare per appartenere al gruppo in parola, supponiamo che si prendano per sostituzioni elementari di I le seguenti

$$B_1\,;\ C_1\,;\quad B_2\,,\ C_2\,;\quad B_3\,,\ C_3\,;\ \ldots \qquad (1)$$

le quali siano così condizionate che gl'esponenti di mutamento scambievoli siano tutti congrui a zero ad eccezione dei seguenti

$$(B_1 C_1) \equiv -(C_1 B_1) \equiv 1\,, \qquad (B_2 C_2) \equiv -(C_2 B_2) \equiv 1\,, \ldots$$

204. Le caratteristiche di queste sostituzioni sono congrue a zero ovvero ad 1, ma possiamo supporre che quelle delle sostituzioni appartenenti ad una medesima coppia siano tra loro congrui: infatti se B_1 e C_1 avessero rispettivamente per carattere 0 ed 1, si potrebbe alla precedente serie sostituire l'altra

$$B_1\,,\ C_1 B_1\,;\quad B_2\,,\ C_2\,;\quad B_3\,,\ C_3\,;\ \ldots$$

nella quale il carattere di $C_1 B_1$ è zero, per essere

$$\text{caratt. } C_1 B_1 \equiv \text{caratt. } C_1 + \text{caratt. } B_1 + (C_1 B_1) \pmod 2,$$

l'esponente di mutamento delle sostituzioni di una coppia è congruo ad 1, mentre quello di due sostituzioni appartenenti a coppie diverse è congruo a zero.

205. Inoltre se ρ è il numero delle coppie della serie (1) le di cui sostituzioni hanno per carattere 1 ed è ρ maggiore di 1, possiamo a questa serie sostituirne un'altra in cui ρ sia 1 ovvero zero. Infatti se i caratteri delle due prime coppie B_1, C_1; B_2, C_2 fossero congrui ad 1, potremmo sostituire alla serie (1) l'altra

$$B_1 B_2 \,,\, C_1 B_2 \;;\quad B_1 C_1 B_2 C_2 \,,\, B_1 C_1 C_2 \;;\quad B_3 \,,\, C_3 \;;$$

nella quale i caratteri delle sostituzioni delle due prime coppie sono congrui a zero, l'esponente di mutamento delle sostituzioni di ciascuna coppia è congruo ad 1 e quello di due sostituzioni appartenenti a coppie diverse, è congruo a zero. Or potendosi sostituire alla serie (1) un'altra analoga in cui il valore di ρ è diminuito di 2; sarà possibile di sostituire alla (1) una serie analoga in cui il valore di ρ sia 1 o zero.

206. Or supponiamo che questa condizione si verifichi nella (1), che x_1, y_1; x_2, y_2; ... x_n, y_n siano gl'indici pei quali si abbia

$$B_1 = (x_1 \,,\, y_1 \ldots x_1 + 1 \,,\, y_1 \ldots) \,, \qquad C_1 = (x_1 \,,\, y_1 \ldots x_1 \,,\, y_1 + 1 \,,\, \ldots) \ldots$$

e che la sostituzione T riferita ai medesimi indici prenda la forma

$$T = \left| \begin{array}{l} x_1 y_1 \;\; a'_1 x_1 + c'_1 y_1 + \ldots + a'_n x_n + c'_n y_n \,,\; b'_1 x_1 + d'_1 y_1 + \ldots + b'_n x_n + d'_n y_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n y_n \;\; a_1^{(n)} x_1 + c_1^{(n)} y_1 + \ldots + a_n^{(n)} x_n + c_n^{(n)} y_n,\; b_1^{(n)} x_1 + d_1^{(n)} y_1 + \ldots + b_n^{(n)} x_n + d_n^{(n)} y_n \end{array} \right|$$

Allora le sostituzioni $B_1, C_1, \ldots$ saranno dalla T trasformate nell'altre

$$B'_1 = B_1^{a'_1} C_1^{b'_1} B_2^{a_{1,2}} C_2^{b_{1,2}} \ldots \,, \qquad C'_1 = B_1^{c'_1} C_1^{d'_1} B_2^{c_{1,2}} C_2^{d_{1,2}} \ldots \,, \ldots \,,$$

quindi esprimendo che l'esponente di mutamento di due qualunque delle sostituzioni B_1, C_1 etc. non si altera se sono trasformate per T si hanno le relazioni

$$\begin{array}{ll} \sum\limits_\mu a_\nu^{(\mu)} d_\nu^{(\mu)} - b_\nu^{(\mu)} c_\nu^{(\mu)} \equiv 1 & \sum\limits_\mu a_\nu^{(\mu)} d_{\nu'}^{(\mu)} - b_\nu^{(\mu)} c_{\nu'}^{(\mu)} \equiv 0 \text{ se } \nu' \gtrless \nu \\ \sum\limits_\mu a_\nu^{(\mu)} b_{\nu'}^{(\mu)} - b_\nu^{(\mu)} a_{\nu'}^{(\mu)} \equiv 0 & \sum\limits_\mu c_\nu^{(\mu)} d_{\nu'}^{(\mu)} - d_\nu^{(\mu)} c_{\nu'}^{(\mu)} \equiv 0 \pmod 2. \end{array} \qquad (1)$$

207. È evidente che la trasformata di una sostituzione

$$S = B_1^\alpha C_1^\beta B_2^\gamma C_2^\delta \ldots$$

di I per T avrà lo stesso carattere di S quante volte lo stesso succede per ciascuna delle sostituzioni elementari B_1, C_1, B_2, C_2 etc. di I, quindi per esprimere la 2ª condizione a cui deve sodisfare T basterà esprimere che il carattere di una qualunque delle sostituzioni B_1, C_1 etc. sia congruo a quello della sua trasformata; il che conduce quando $\rho = 0$ alle relazioni

$$a'_\mu b'_\mu + \ldots + a_\mu^{(n)} b_\mu^{(n)} \equiv 0 \,, \qquad c'_\mu d'_\mu + \ldots + c_\mu^{(n)} d_\mu^{(n)} \equiv 0 \qquad (2)$$

nelle quali bisogna dare a μ successivamente i valori $1 \cdot 2 \ldots n$, e quando $\rho = 1$ all'altre

$$a'_1 b'_1 + a''_1 b''_1 + \dots + a'_1 + b'_1 \equiv c'_1 d'_1 + c''_1 d''_1 + \dots + c'_1 + d'_1 \equiv 1$$

$$a'_\mu b'_\mu + a''_\mu b''_\mu + \dots + a'_\mu + b'_\mu \equiv c'_\mu d'_\mu + c''_\mu d''_\mu + \dots + c'_\mu + d'_\mu \equiv 0 \text{ (se } \mu > 1). \tag{3}$$

208. Potendosi determinare i coefficienti a'_1, b'_1 etc. o col sistema di relazioni (1) e (2) ovvero coll'altro (1) e (3) si hanno due gruppi diversi che si chiamano *ipo-abelliani* e per distinguere l'uno dall'altro si chiama di *prima specie* quello relativo alle (2) e di *seconda specie* quello relativo alle (3).

209. Teorema 1.° – *L'ordine del gruppo ipo-abelliano* H_0 *di prima specie è uguale ad*

$$\omega_n = (P_n - 1)\, 2^{2n-2} \dots (P_2 - 1)\, 2^2 \cdot 2,$$

indicando con P_n *il numero delle soluzioni della congruenza*

$$a_1 b_1 + a_2 b_2 + \dots + a_n b_n \equiv 0 \pmod 2.$$

Infatti ogni sostituzione di questo gruppo che scambia x_1 in $f = a'_1 x_1 + c'_1 y_1 + \dots + a'_{2n} x_n + c'_n y_n$ si può mettere sotto la forma $\Sigma_1 \Sigma$, essendo Σ una sostituzione che scambia x_1 in f e Σ_1 un'altra sostituzione che non altera x_1, quindi ω_n sarà uguale al numero delle possibili funzioni f moltiplicato per l'ordine ω' del gruppo H'_0 formato dalle sostituzioni Σ_1. Ora ogni sostituzione di H'_0 che scambia y_1 in $f_1 = b'_1 x_1 + d'_1 y_1 + \dots + b'_n x_n + d'_n y_n$ si può porre sotto la forma $\Sigma'_1 \Sigma'$, indicando con Σ'_1, una sostituzione di H'_0 che non altera y_1 ed x_1 e con Σ' un'altra sostituzione dello stesso gruppo che pone f' in luogo di y_1, quindi ω' sarà uguale al numero delle diverse funzioni f_1 moltiplicato per l'ordine ω_{n-1} del gruppo H''_0 formato dalle sostituzioni Σ'_1. Ma dovendo essere $d'_1 \equiv 1$, come si è mostrato nel paragrafo (197), ed essendo

$$b'_1 + b'_2 d'_2 + \dots + b'_n d'_n \equiv 0,$$

dei coefficienti di f_1 solo b'_1 e d'_1 sono determinati e ciascuno degl'altri può prendere i valori 1 e 0, ma questi coefficienti sono $2n-2$, quindi si possono avere 2^{2n-2} funzioni f_1 diverse, e per conseguenza sarà $\omega' = 2^{2n-2}\omega_{n-1}$. Ma con un ragionamento analogo a quello fatto nel paragrafo (197), si prova che H''_0 è il gruppo ipo-abelliano di 1ª specie di grado 2^{2n-2}, quindi sarà

$$\omega_{n-1} = (P_{n-1} - 1)\, 2^{2n-4}\, \omega_{n-2},$$

e seguitando a fare questa riduzione si perverrà al gruppo ipo-abelliano di 1ª specie di grado 2^2 il di cui ordine sarà uguale a $(P_2 - 1)\, 2^2$ moltiplicato per l'ordine del gruppo formato dalle sostituzioni di H_0 che alterano solo x_n ed y_n, ma questo gruppo è costituito dalla sostituzione 1 e dall'altra

$$(x_1, y_1 \dots x_n, y_n \quad x_1, y_1 \dots y_n \quad -x_n)$$

adunque resta dimostrata la formola proposta.

210. Teorema 2.° – *L'ordine* ω'_n *del gruppo ipo-abelliano di seconda specie* H_1 *è uguale ad*

$$\omega'_n = (2^n - P_n)\, 2\, P_{n-1}\, \omega'_{n-1}.$$

Infatti ogni sostituzione di questo gruppo che pone $f = a'_1 x' + c'_1 y_1 + \dots + a'_n x_n + c'_n y_n$ in luogo di x_1 si può porre sotto la forma $\Sigma_1 \Sigma$, essendo Σ una sostituzione di H_1

che scambia x_1 con f e Σ_1 un'altra sostituzione di H_1 che non altera x_1, quindi ω'_n sarà uguale al prodotto del numero delle diverse funzioni f per l'ordine ω' del gruppo H'_1 formato dalle sostituzioni Σ_1. Ma se si esprime che T^{-1} sia anche una sostituzione di H_1 si avranno delle relazioni analoghe a quelle stabilite per questo gruppo, tra le quali vi sono le seguenti

$$b'_1 d'_1 + b'_2 d'_2 + \dots + b'_1 + d'_1 \equiv 1 \qquad (4)$$

$$a'_1 c'_1 + \dots + a'_n c'_n + a'_1 + c'_1 \equiv 0 \qquad (5)$$

la 2ª delle quali potendo esser posta sotto la seguente forma

$$(a'_1 + 1)(c'_1 + 1) + \dots + a'_n c'_n \equiv 1$$

è sodisfatta da $2^{2n} - P_n$ sistemi di valori di $a'_1 + 1$, $c'_1 + 1$, ... a'_n, c'_n e quindi da altrettanti sistemi di valori di a'_1, c'_1 ... a'_n. c'_n. adunque vi saranno $2^{2n} - P_n$ funzioni f diverse e per conseguenza sarà

$$\omega_n = (2^{2n} - P_n)\,\omega'.$$

Analogamente ogni sostituzione di H'_1 che scambia y_1 con $f_1 = b'_1 x_1 + d'_1 y_1 + \dots$ $\dots + b'_n x_n + d'_n y_n$ si può porre sotto la forma $\Sigma'_1 \Sigma'$, essendo Σ' una sostituzione di H'_1 che pone f_1 in luogo di y_1 e Σ'_1 un'altra sostituzione dello stesso gruppo che non altera x_1 ed y_1, quindi ω' sarà uguale al prodotto del numero delle diverse funzioni f_1 per l'ordine del gruppo formato dalle sostituzioni Σ'_1, ma questo gruppo è appunto il gruppo ipo-abelliano di 2ª specie di grado 2^{2n-2}, il di cui ordine è indicato da ω'_{n-1}, ed il numero delle diverse funzioni f_1 è $2P_{n-1}$, poichè dovendo essere $d' \equiv 1$ (197) la (4) si riduce all'altra

$$b'_2 d'_2 + \dots + b'_n d'_n \equiv 0$$

la quale è sodisfatta da P_{n-1} sistemi di valori di b''_2, d'_2 etc. e b'_1 può prendere i valori 0 ed 1; quindi sarà $\omega' = 2P_{n-1}\,\omega'_{n-1}$ e sostituendo sarà $\omega_n = (2^{2n} - P_n) 2P_{n-1}\,\omega'_{n-1}$.

211. Con ragionamenti analoghi a quello seguito per dimostrare il teorema 3° (199) si dimostrerebbe che ogni sostituzione del 1° gruppo abelliano è derivato dalle sole sostituzioni M_μ, $N_{\mu,\nu}$; e che ogni sostituzione del 2° gruppo abelliano è derivato dalle precedenti essendo μ e $\nu > 1$, e dall'altre

$$L_1 = (x_1\,,\, y_1 \dots x_1 + y_1\,,\, y_1\,,\, \dots)\,, \qquad M_1 = (x_1\,,\, y_1\,,\, \dots y_1\,,\, x_1\,,\, \dots)$$

$$U = (x_1\,,\, y_1\,,\, x_2\,,\, y_2\,,\, \dots x_2 + y_2\,,\;\; y_1 + y_2\,,\;\; x_1 + x_2 + y_2\,,\;\; x_1 + y_1 + x_2 + y_2\,,\, \dots)$$

CAPO 12.°

Fasci Abelliani ed Ipo-abelliani.

212. Indichiamo con F un fascio di sostituzioni tra loro mutabili contenuto nel gruppo Abelliano H di grado p^{2n}, e supponiamo che il gruppo G contenuto in H e permutabile ad F sia primario. Allora non vi saranno delle funzioni y, y'...... degl'indici in numero minore di quest'indici che saranno scambiate da ogni sostituzione di G con funzioni di y, y', etc. e quindi non esisteranno di queste funzioni

per le sostituzioni del gruppo G' permutabile ad F e contenuto nel gruppo lineare di grado p^{2n}; laonde G' sarà primario e vi sarà un sistema d'indici per cui tutte le sostituzioni di F potranno essere ridotte alla loro forma canonica. Quest'indici si divideranno come è indicato nel teorema 4° (51) e formeranno una sola classe, perchè se ne formassero più d'una, scambiando quest'indici in altri reali, quest'ultimi sarebbero divisi allo stesso modo degl'immaginari, e gl'indici di una stessa classe sarebbero scambiati con funzioni dei medesimi indici ed il gruppo G' non sarebbe primario.

213. Diremo *congiunte* due serie d'indici $X, X', \ldots$; $Y, Y', \ldots$, se chiamando α e β i fattori per cui una sostituzione S di F moltiplica rispettivamente gl'indici dell'indicate serie e con m il fattore per cui S moltiplica l'esponente di mutamento delle sostituzioni C_X, C_Y, corrispondenti ad X e ad Y, si abbia la relazione $\alpha\beta \equiv m \pmod{p}$.

Teorema 1.° — *Ogni serie d'indici ha la sua congiunta.*

Ritenendo le precedenti denominazioni, si ha che le trasformate di C_X e di C_Y per S sono rispettivamente C_X^{α} e C_Y^{β}, quindi il loro esponente di mutamento è $\alpha\beta(C_X, C_Y)$, ma S moltiplica per m l'esponente di mutamento di C_X e C_Y, dunque si avrà la relazione $\alpha\beta(C_X, C_Y) \equiv m(C_X, C_Y)$, la quale può aver luogo o quando $(C_X, C_Y) \equiv 0$, ovvero quando $\alpha\beta \equiv m$, ma la prima non ha luogo per tutte le sostituzioni C_Y, altrimenti sarebbero uguali a zero gl'esponenti di mutamento di C_X e di tutte le sostituzioni derivate da $C_X, C_Y, \ldots$; $C_{X'}, C_{Y'} \ldots$; ... il che è contro l'ipotesi; adunque vi dovrà essere una sostituzione C_Y per cui si abbia $(C_X, C_Y) \gtrless 0 \pmod{p}$ e quindi $\alpha\beta \equiv m$, laonde la serie $X, X' \ldots$ sarà congiunta all'altra $Y, Y', \ldots$.

214. Teorema 2.° — *Se le serie $X, X', \ldots$; $Y, Y', \ldots$ sono congiunte, lo saranno anche le loro conjugate $X_r, X'_r, \ldots$; $Y_r, Y'_r, \ldots$ che si ottengono ponendo i^{p^r} in luogo dell'immaginario i che entra nell'espressioni degl'indici delle prime serie.*

Invero se la sostituzione S moltiplica X ed Y rispettivamente per α e per β, moltiplicherà X_r ed Y_r rispettivamente per α^{p^r} e β^{p^r}, ma se nella relazione $\alpha\beta \equiv m$, che ha luogo per essere la serie $X, X', \ldots$ congiunta all'altra $Y, Y', \ldots$, si pone i^{p^r} in luogo di i si ha $\alpha^{p^r}\beta^{p^r} \equiv m^{p^r} \equiv m$, per essere m reale, dunque le due serie $X_r, X'_r, \ldots, \ldots$; $Y_r, Y'_r, \ldots$ sono congiunte.

Corollario. — Se due serie congiunte appartengono al medesimo sistema, le serie di questo sistema sono a due a due congiunte tra loro; e se due serie congiunte appartengono a sistemi diversi ogni serie dell'uno avrà la sua congiunta nell'altro; poichè se nell'espressione di un'indice si pono i^{p^r} in luogo di i si ha un indice che appartiene al medesimo sistema.

215. Teorema 3.° — *Una serie, avrà la sua congiunta o nel medesimo suo sistema, o in un altro o si confonde con sè stessa, secondochè uno di questi casi succede per una serie determinata.*

Siano $X, X' \ldots$; $Y, Y', \ldots$ due serie congiunte ed S una sostituzione di G che

scambia quest'indici con funzioni lineari degl'indici delle nuove serie Z , Z', ... ; U , U', ... Queste ultime serie saranno congiunte. Infatti se non lo fossero F conterrebbe una sostituzione T che moltiplicherebbe gl'indici di queste due serie per dei fattori γ e δ che non sodisferebbero alla relazione $\gamma\delta \equiv m$, essendo m il fattore per cui T moltiplica gl'esponenti di mutamento; ora la sostituzione STS^{-1} moltiplica altresì gl'esponenti di mutamento per m e moltiplica gl'indici delle serie X . X', ... ; Y, Y', ... rispettivamente per γ e δ, quindi queste serie non sarebbero congiunte, il che è contrario all'ipotesi.

Or se due serie congiunte X , X', ... ; Y , Y', ... appartengono allo stesso sistema Σ, dovendo G essere transitivo per essere primario, vi sarà in G una sostituzione S' che scambia gl'indici X, X', ... con funzioni lineari degl'indici di una serie Z , Z', ... di un sistema qualunque Σ' e gl'indici Y, Y', ... con funzioni lineari degl'indici di un'altra serie U, U', ... appartenente a Σ' e quindi la serie Z , Z', ... sarà congiunta all'altra U , U', ...

Che se le due serie congiunte X , X', ... ; Y , Y', ... appartengono a sistemi diversi Σ , Σ', vi sarà una sostituzione di G che scambierà X , X', ... con funzioni lineari degl'indici di una serie Z , Z', ... appartenente ad un sistema qualunque Σ', e gl'indici Y, Y', ... con funzioni lineari degl'indici di una serie U , U', ... appartenente ad un sistema Σ'' diverso da Σ', e sarà la serie Z , Z', ... congiunta all'altra U , U', ...

Infine se una serie è congiunta a sè stessa, avverrà lo stesso per qualunque altra, poichè se una serie non si confondesse colla sua congiunta, per ciò che precede, ogni serie dovrebbe essere distinta dalla sua congiunta.

Il fascio F si dice di 1ª o di 2ª o di 3ª categoria secondochè una serie ha la sua congiunta in un sistema diverso da quello a cui essa appartiene, o nello stesso suo sistema, o coincide con sè stessa.

216. Teorema 4.° – *Affinchè il fascio F appartenga ad uno dei due gruppi ipo-abelliani è necessario e sufficiente che siano uguali a zero i caratteri delle sostituzioni* C_X , C_Y , ...

Sia S una sostituzione di F la quale moltiplichi gl'indici X , Y, ... rispettivamente per α_1 β_1 ... Allora S trasformerà C_X, C_Y ... rispettivamente in C_X^{α}, C_Y^{β}, ... e quindi moltiplicherà i caratteri C_X , C_Y ... rispettivamente per α, β, ... , ma se S è ipo-abelliana i caratteri di C_X , C_Y , ... non debbono essere alterati per effetto della trasformazione, dunque o i fattori α, β, ... sono tutti congrui ad 1, o alcuni di essi sono congrui ad 1, o i caratteri delle sostituzioni C_X , C_Y ..... sono tutti uguali a zero; ma se tutti i fattori α, β, ... sono congrui ad 1 il fascio F si riduce ad 1, il che non è; se α è diverso da 1 il carattere di C_X si annulla, e siccome in G vi deve essere una sostituzione che moltiplica un'altro indice qualunque Y per α (164), sarà il carattere di C_Y congruo a zero, quindi i caratteri di C_X, C_Y, ... debbono essere congrui a zero.

È poi evidente che questa condizione sia sufficiente.

CAPO 13.°

Metodi generali per formare dei gruppi parziali contenuti nel gruppo lineare.

1.° METODO.

217. Indichiamo con $F(x_1, y_1 \ldots\ldots; x_2, y_2 \ldots; \ldots)$ una funzione di più indici $x_1, y_1 \ldots; x_2, y_2 \ldots; \ldots$ variabili da 0 a $p-1$, e divisi in serie formate dallo stesso numero d'indici. Se esistono delle sostituzioni lineari che operate sopra ciascuna serie d'indici trasforma la proposta funzione nel prodotto della stessa funzione per una costante, queste sostituzioni formeranno un gruppo. Infatti se S ed S' sono due sostituzioni le quali trasformano F rispettivamente in mF ed in $m'F$, l'altra SS' trasformerà F in $m'mF$, quindi l'assieme dell'indicate sostituzioni comprenderà il prodotto di due qualunque di esse, e perciò costituirà un gruppo.

218. Supponiamo che gl'indici si dividano in m serie ciascuna formata di mn indici, e che gl'indici di ciascuna serie si dividano in n sistemi ciascuno formato da m indici; allora indicando con

$$x_\mu^{(1)}, y_\mu^{(1)} \ldots; \quad x_\mu^{(2)}, y_\mu^{(2)} \ldots; \ldots; \quad x_\mu^{(n)}, y_\mu^{(n)} \ldots$$

gli n sistemi della μ^{ma} serie, possiamo porre

$$F = \sum_{\nu=1}^{\nu=n} \begin{vmatrix} x_1^{(\nu)}, y_1^{(\nu)} \ldots\ldots\ldots\ldots \\ x_2^{(\nu)}, y_2^{(\nu)} \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_m^{(\nu)}, y_m^{(\nu)} \ldots\ldots\ldots\ldots \end{vmatrix}.$$

Indi facciamo subire agl'elementi di ciascuna linea di ciascun determinante la sostituzione

$$S = (x, y, z, \ldots\ ax + by + cz + \ldots,\ \ a'x + b'y + c'z + \ldots,\ \ a''x + b''y + c''z + \ldots, \ldots).$$

Avremo così una somma di determinanti ad elementi polinomii, e scomponendoli in altri ad elementi monomii, alcuni di questi si annulleranno, altri saranno uguali a quelli contenuti in F moltiplicati per costanti, ed altri diversi dal già detti anche moltiplicati per costanti. Allora se intendiamo raccolti in un solo tutt'i termini che contengono lo stesso determinante, uguagliando ad m il moltiplicatore di ciascun determinante contenuto in F, ed a zero quello di ciascun determinante non contenuto in F, si avranno le relazioni a cui dovranno sodisfare le costanti $a, b, \ldots$ perchè S moltiplicasse F per m.

219. Onde meglio dichiarare quanto abbiamo detto, supponiamo che si abbiano le due serie d'indici

$$x_1, y_1; \ x_2, y_2; \ldots\ldots x_n, y_n$$
$$\varepsilon_1, \eta_1; \ \varepsilon_2, \eta_2; \ldots\ldots \varepsilon_n, \eta_n$$

e che ciascuna si divida in n sistemi formati da 2 indici. In questo caso sarà

$$F = \sum_{\nu=1}^{\nu=n} \begin{vmatrix} x_\nu & y_\nu \\ \varepsilon_\nu & \eta_\nu \end{vmatrix},$$

ed operando sopra gl'indici di ciascuna serie la sostituzione

$$S = \begin{vmatrix} x_1 & a'_1 x_1 + c'_1 y_1 + \ldots + a'_n x_n + c'_n y_n \\ y_1 & b'_1 x_1 + d'_1 y_1 + \ldots + b'_n x_n + d'_n y_n \\ \cdots & \cdots\cdots\cdots\cdots\cdots\cdots \\ x_n & a_1^{(n)} x_1 + c_1^{(n)} y_1 + \ldots + a_n^{(n)} x_n + c_n^{(n)} y_n \\ y_n & b_1^{(n)} x_1 + d_1^{(n)} y_1 + \ldots + b_n^{(n)} x_n + d_n^{(n)} y_n \end{vmatrix}$$

si avrà

$$F' = \sum_{\nu=1}^{\nu=n} \begin{vmatrix} a_1^{(\nu)} x_1 + c_1^{(\nu)} y_1 + \ldots + a_n^{(\nu)} x_n + c_n^{(\nu)} y_n, & b_1^{(\nu)} x_1 + d_1^{(\nu)} y_1 + \ldots + b_n^{(\nu)} x_n + d_n^{(\nu)} y_n \\ a_1^{(\nu)} \varepsilon_1 + c_1^{(\nu)} \eta_1 + \ldots + a_n^{(\nu)} \varepsilon_n + c_n^{(\nu)} \eta_n, & b_1^{(\nu)} \varepsilon_1 + d_1^{(\nu)} \eta_1 + \ldots + b_n^{(\nu)} \varepsilon_n + d_n^{(\nu)} \eta_n \end{vmatrix}.$$

e scomponendo ogni determinante in altri ad elementi monomii si avrà

$$F' = \sum_{\mu=1}^{\mu=n} \sum_{\nu=1}^{\nu=n} \begin{vmatrix} a_\mu^{(\nu)} & b_\mu^{(\nu)} \\ c_\mu^{(\nu)} & d_\mu^{(\nu)} \end{vmatrix} \begin{vmatrix} x_\mu & y_\mu \\ \varepsilon_\mu & \eta_\mu \end{vmatrix} + \sum_{\rho=1}^{\rho=n} \sum_{\mu=1}^{\mu=n} \sum_{\nu=1}^{\nu=n} \begin{vmatrix} a_\mu^{(\nu)} & a_\rho^{(\nu)} \\ b_\mu^{(\nu)} & b_\rho^{(\nu)} \end{vmatrix} \begin{vmatrix} x_\mu & x_\rho \\ \varepsilon_\mu & \varepsilon_\rho \end{vmatrix}$$

$$+ \sum_{\rho=1}^{\rho=n} \sum_{\mu=1}^{\mu=n} \sum_{\nu=1}^{\nu=n} \begin{vmatrix} c_\mu^{(\nu)} & c_\rho^{(\nu)} \\ d_\mu^{(\nu)} & d_\rho^{(\nu)} \end{vmatrix} \begin{vmatrix} y_\mu & y_\rho \\ \eta_\mu & \eta_\rho \end{vmatrix} + \sum_{\rho'=1}^{\rho'=n} \sum_{\mu'=1}^{\mu'=n} \sum_{\nu=1}^{\nu=n} \begin{vmatrix} a_{\mu'}^{(\nu)} & b_{\mu'}^{(\nu)} \\ c_{\rho'}^{(\nu)} & d_{\rho'}^{(\nu)} \end{vmatrix} \begin{vmatrix} x_{\mu'} & y_{\rho'} \\ \varepsilon_{\mu'} & \eta_{\rho'} \end{vmatrix}$$

essendo $\rho' \gtrless \mu'$.

Quindi le condizioni a cui debbono sodisfare le costanti che entrano in S affinchè questa sostituzione moltiplichi F per m saranno

$$\sum_{\mu=1}^{\mu=n} \sum_{\nu=1}^{\nu=n} \begin{vmatrix} a_\mu^{(\nu)} & b_\mu^{(\nu)} \\ c_\mu^{(\nu)} & d_\mu^{(\nu)} \end{vmatrix} \equiv m, \quad \sum_{\rho=1}^{\rho=n} \sum_{\mu=1}^{\mu=n} \sum_{\nu=1}^{\nu=n} \begin{vmatrix} a_\mu^{(\nu)} & a_\rho^{(\nu)} \\ b_\mu^{(\nu)} & b_\rho^{(\nu)} \end{vmatrix} \equiv 0$$

(mod p

$$\sum_{\rho=1}^{\rho=n} \sum_{\mu=1}^{\mu=n} \sum_{\nu=1}^{\nu=n} \begin{vmatrix} c_\mu^{(\nu)} & c_\rho^{(\nu)} \\ d_\mu^{(\nu)} & d_\rho^{(\nu)} \end{vmatrix} \equiv 0, \quad \sum_{\rho'=1}^{\rho'=n} \sum_{\mu'=1}^{\mu'=n} \sum_{\nu=1}^{\nu=n} \begin{vmatrix} a_{\mu'}^{(\nu)} & b_{\mu'}^{(\nu)} \\ c_{\rho'}^{(\nu)} & d_{\rho'}^{(\nu)} \end{vmatrix} \equiv 0.$$

Queste relazioni sono equivalenti a quelle già trovate per le sostituzioni che compongono il gruppo di Abel.

220. Il metodo testè esposto è dovuto a Kronecher, e può essere generalizzato come apparirà da quanto segue:

Siano φ una funzione razionale ed omogenea degl'indici $x_1\, y_1 \ldots;\ x_2\, y_2 \ldots;\ \ldots,$ ψ una funzione qualunque degli stessi indici e dei coefficienti di φ, φ' e ψ' le trasformate di φ e di ψ per mezzo di una sostituzione lineare S operata sopra ciascuna serie d'indici. Se ψ' si compone per mezzo degl'indici e dei coefficienti di φ' come ψ si compone per mezzo degl'indici e dei coefficienti di φ, diciamo che ψ sia un *covariante* di φ per rispetto alla sostituzione S. Se ψ fosse indipendente dagl'indici diciamo che ψ sia un *invariante* di φ per rispetto alla sostituzione S.

Ora è evidente che se S, S', S'' etc. sono delle sostituzioni rispetto a cui ψ sia un *covariante* o un *invariante* di φ, il loro insieme formerà un gruppo perchè ψ sarà un *covariante* o un *invariante* per rispetto al prodotto di due qualunque di esse.

221. Supponiamo che sia

$$\varphi = \theta x + \theta_1 y\,, \qquad \psi = l\theta^2 + 2m\,\theta\theta_1 + n\theta_1^2.$$

Operando su φ la sostituzione

$$S = (x\,,\,y\,,\quad ax + by\,,\quad a'x + b'y)$$

si ha

$$\varphi' = (a\theta + a'\theta_1)\,x + (b\theta + b'\theta_1)\,y$$

e l'espressione composta coi coefficienti di φ' come ψ si compone con quelli di φ è

$$\psi' = l\,(a\theta + a'\theta_1)^2 + 2m\,(a\theta + a'\theta_1)\,(b\theta + b'\theta_1) + n\,(b\theta + b'\theta_1)^2$$
$$= (la^2 + 2mab + nb^2)\,\theta^2 + 2\,(laa' + mab' + ma'b + nbb')\,\theta\theta_1 + (la'^2 + ma'b' + nb'^2)\,\theta_1^2.$$

Quindi perchè ψ sia un *invariante* di φ è necessario che si abbia

$$l \equiv la^2 + 2mab + nb^2$$
$$m \equiv laa' + mab' + ma'b + nbb'$$
$$n \equiv la'^2 + 2ma'b' + nb'^2.$$

Ora avendosi tre congruenze tra le quattro ignote a, b, a', b', possiamo esprimere tre di esse p. e. a, b, a' in funzione della quarta b' e delle costanti l, m, n. Formando il determinante di S col dare ad a, b, a' i loro valori espressi in funzione di b', si darebbero a b' tutt' i valori pei quali questo determinante fosse primo col modulo p, le sostituzioni che ne risulterebbero formerebbero un gruppo che corrisponderebbe al sistema di valori assunti per l, m, n.

222. Se supponiamo $l \equiv 1$, $m \equiv 0$, $n \equiv 0$, le tre congruenze sarebbero indipendenti da b e da b', e sarebbe $a \equiv \pm 1$ ed $a' \equiv 0$; ed il tipo delle sostituzioni che formano il gruppo corrispondente a questo sistema di valori di l, m, n sarebbe

$$S = (x\,,\,y\,,\quad \pm x + by\,,\quad b'y).$$

Si avrebbero le singole sostituzioni del gruppo dando a b ed a b' tutt' i valori pei quali il determinante

$$\begin{vmatrix} \pm 1 & b \\ 0 & b' \end{vmatrix}$$

risulta primo con p.

223. Se poniamo

$$\varphi = \theta x + \theta_1 y\,, \qquad \psi = (m\theta + n\theta_1)\,x + (m'\theta + n'\theta_1)\,y$$

le trasformate per mezzo di S saranno

$$\varphi' = (a\theta + a'\theta_1)\,x + (b\theta + b'\theta_1)\,y$$

$$\psi' = [(am + a'm')\,\theta + (an + a'n')\,\theta_1]\,x + [(bm + b'm')\,\theta + (bn + b'n')\,\theta_1]\,y\,,$$

quindi per essere ψ un covariante di φ per rispetto ad S è necessario che si abbia

$$a'm' \equiv nb\,, \quad an + a'n' \equiv ma' + nb'\,, \quad bm + b'm' \equiv am' + bn'\,;$$

e poichè la 3ª di queste relazioni è una conseguenza delle altre due, ponendo $m' = kn$, $m - n' = \lambda n$, si avrà dalle due prime

$$b = ka'\,, \qquad b' = a - \lambda a'\,,$$

quindi il tipo delle sostituzioni che compongono il gruppo corrispondente ad un dato sistema di valori di k e λ sarà

$$S = [x\,, y\,, \quad ax + ka'y\,, \quad a'x + (a - \lambda a')\,y].$$

Si otterranno tutte le sostituzioni di uno stesso gruppo dando ad a e ad a' tutt'i valori per cui il determinante

$$\begin{vmatrix} a & ka' \\ a' & a - \lambda a' \end{vmatrix}$$

risulta primo col modulo.

2.° METODO.

224. Se si hanno una funzione omogenea di più sistemi d'indici $x_1\,, y_1\,, \ldots\,;$ $x_2\,, y_2\,, \ldots\,; \ldots$ ed un gruppo di sostituzioni lineari per ciascun sistema, trasformando la funzione coll'operare sopra ciascun sistema d'indici una sostituzione del gruppo corrispondente, la trasformata avrà evidentemente la medesima forma della proposta, ed i coefficienti della trasformata saranno funzioni dei coefficienti della proposta e delle costanti che entrano nell'espressioni della sostituzione adoperata nella trasformazione. Di qui risulta che la trasformata possa anche ottenersi colla sostituzione lineare che abbia per scopo di cambiare i coefficienti della proposta nei corrispondenti della trasformata.

Ora l'assieme delle sostituzioni di questo genere che si possono ottenere combinando in tutt'i modi possibili le sostituzioni dei gruppi dati formerà un gruppo G. Infatti se $S', S'', S''', \ldots\ldots;$ $S_1\,, S_2\,, S_3\,, \ldots\ldots$ sono due serie di sostituzioni prese nei dati gruppi, la sostituzione g tra i coefficienti corrispondente all'altra $S'S_1\,S''S_2S'''S_3\ldots$ sarà identica all'altra g' che corrisponde ad $S'S''S'''\ldots S_1S_2S_3\ldots$, ma g appartiene a G perchè $S'S_1\,, S''S_2\,, S'''S_3\,, \ldots.$ sono sostituzioni dei gruppi dati, dunque anche g' appartiene a G, ma g' è il prodotto delle sostituzioni tra i coefficienti corrispondenti alle sostituzioni $S'S''S'''\ldots$, $S_1S_2S_3\ldots$, dunque G contiene il prodotto di due qualunque delle sue sostituzioni, epperò è un gruppo.

225. Onde meglio dichiarare ciò che si è detto in generale aggiungiamo i seguenti esempii.

Siano $$\varphi = \theta_0 x\varepsilon + \theta_1 x\eta + \theta_2 y\varepsilon + \theta_3 y\eta$$

una funzione omogenea per rispetto alle due serie d'indici $x\,, y\,;\ \varepsilon\,, \eta$ ed

$$S = (x\,, y \quad ax + by \quad a'x + b'y)\,, \qquad \Sigma = (\varepsilon\,, \eta \quad \alpha\varepsilon + \beta\eta\,. \quad \alpha'\varepsilon + \beta'\eta)$$

due sostituzioni appartenenti a due gruppi G e Γ.

Operando queste sostituzioni sulla φ, si avrà una trasformata la quale si otterrebbe ancora se sulle θ contenute in φ si operasse la sostituzione

$$\Delta = \begin{vmatrix} \theta_0 & a\alpha\theta_0 + a\alpha'\theta_1 + a'\alpha\theta_2 + a'\alpha'\theta_3 \\ \theta_1 & a\beta\theta_0 + a\beta'\theta_1 + a'\beta\theta_2 + a'\beta'\theta_3 \\ \theta_2 & b\alpha\theta_0 + b\alpha'\theta_1 + b'\alpha\theta_2 + b'\alpha'\theta_3 \\ \theta_3 & b\beta\theta_0 + b\beta'\theta_1 + b'\beta\theta_2 + b'\beta'\theta_3 \end{vmatrix}.$$

Tutte le sostituzioni Δ che si ottengono combinando tutte le sostituzioni di G con tutte quelle di Γ formeranno un gruppo.

226. Sia inoltre $$\varphi = \theta x + \theta' y + \ldots$$

una funzione lineare di una sola serie d'indici $x, y, \ldots$. Operandovi la sostituzione

$$S = (x, y, \ldots \quad ax + by + \ldots \quad a'x + b'y + \ldots)$$

si otterrà una trasformata la quale risulterebbe anche operando sulle θ la sostituzione

$$\Delta = (\theta, \theta', \ldots \quad a\theta + a'\theta' + \ldots, \quad b\theta + b'\theta' + \ldots)$$

la quale si ottiene da S scambiando fra loro i coefficienti simmetrici per rapporto alla diagonale del determinante di S o cambiando gl'indici, donde il teorema:

Teorema. — *Essendo dato un gruppo di sostituzioni lineari, se ne dedurrà un altro permutando tra loro, in ciascuna delle sue sostituzioni, i coefficienti simmetrici l'uno all'altro per rapporto alla diagonale del determinante della sostituzione che si considera.*

FINE.

p.	v.	ERRATA	CORRIGE
8	26	$S_1, S_2 \ldots$	$S, S_1, \ldots$
»	31	S_1, S_2	S, S_1
9	14	k	$\frac{k}{p}$
»	37	U	M
11	16	V	γ
12	6	$(\varepsilon\varphi\rho)$	$(\varepsilon\rho\varphi)$
15	28	$m-3$	$2n-3$
»	29	sostituzioni che	sostituzione T che
25	8	sono $\frac{N}{l}$	sono N, $\frac{N}{l}$
26	15	debbono	non debbono
»	36	$g_\delta h_\gamma h'_{\gamma'} k_\alpha$	$g_\delta h_\gamma h'_{\gamma'} i_\beta k_\alpha$
»	»	»	»
31	3	(4)	(5)
34	20	$\lambda_{\mu-1} x^{m-2}$	$\lambda_{\mu-2} x^{\mu-2}$
35	4	y	x
36	16	V	γ
»	34	$A_n U_n$	$A_n B_n$
37	19	G	H
38	25	(58. Co 61)	(58, 61)
41	18	$n-1$	$n+1$
»	19	$k-n+1$	$k-n-1$
42	12	per mezzo di A'''	per mezzo di A'''^{-1}
»	15	$A'''A''$	$(A'''A'')^{-1}$
43	8	il 1°	il 2°
»	9	il 2°	il 1°
»	11	$(k-\mu-\nu)$	$(k-\mu-\nu+1)$
»	32	di $\varphi(k-\nu)$	summultiplo di $\varphi(k-\nu)$
44	18	(56)	(55)
»	22	μ	μ'
45	1	$\alpha'=k'-\mu'-n-\nu-\alpha_1-\alpha_2$.	$\alpha'=k'-\mu'-n+\alpha_1+\alpha_2$.
»	17	è α''	ed essendo α'' il massimo dei numeri α'', α'_1, α''_2 etc. è $\alpha''_1+\alpha''_2>$
40	31	multiplo	summultiplo
47	5	$k<7$	$k>7$
»	34	$\overset{=}{<} 3$	$\overset{=}{>} 3$
»	36	$k<7$	$k>7$
48	17	valori	valori, se $k>12$
49	23	$\frac{k}{4}$	$\frac{k}{2}$
»	26	$k-5$	$k-9$
50	34	$k<12$	$k>12$
51	24	(33...)	(31...)
»	28	B_1	B
52	34	L'ordine di H	L'ordine di H'
53	19	$\frac{2\nu-3}{q}\nu$	$\left(\frac{2\nu-3}{q}-1\right)\nu$
»	21	$2\nu \overset{=}{<} n$	$3\nu \overset{=}{<} n$
»	33	$A'B'$	$(A'B')^{-1}$
54	12	non sposta x_1, x_2	ed A^2 equivale ad un numero pari di trasposizioni fatte su di x_1, x_2 etc.
56	9	$A'B'H'G$	$(A'B'H'G)^{-1}$
»	33	$A'B'$	$(A'B')^{-1}$
57	7	(33)	(32. Co)
59	24	(85)	(86)
60	11	lo sarà	non lo sarà
»	12	seguito	seguito ed $(x_1..x_p)$ equi-
»	»		vale ad $(F_1...F_p)$
68	10	$ip^{\nu-1}$	$i^{p^{\nu-1}}$
69	19	la radice	radice
74	35	$p+1$	$p-1$
76	22	$\frac{p-1}{4}$	$\frac{p-1}{2}$
79	2	$\Sigma[\varphi(0)^m+\ldots]$	$\varphi(0)^m+\ldots+\varphi(p-1)^m$
90	21	$c=1$	$c=-1$
»	24	αy, $\alpha^{-1}y$	$\alpha y'$, $-\alpha^{-1}y$
»	27	$z=h\,dy$	$z=4\,dy$
91	8	$2y'+y$	$2y'-y$
97	4	I'	H_2
»	»	I'	H'
116	30	$i^{p^{\rho(r-1)}}$	$i^{p^{\rho(\nu-1)}}$
121	28	(mod p)	(mod μ)
132	20	$S'^2=T_1$	$S'^6=T_1$


BIBLIOTECA